Departamento de Ingeniería Telemática

PROYECTO FIN DE CARRERA

ESTUDIO DE UN SISTEMA REDIRECTOR DE TRÁFICO DE ITINERANCIA INTERNACIONAL EN REDES 4G

Autor: Marta López Sánchez

Tutor: Victor Corcoba y Mario Muñoz

Leganés, Septiembre de 2015

Título: Estudio de un sistema redirector de tráfico de itinerancia internacional en redes 4G
Autor: Marta López Sánchez
Director: Victor Corcoba y Mario Muñoz

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de Septiembre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Quiero dar las gracias a mis tutores Mario y Víctor, por acompañarme y guiarme en el cierre de una etapa importante en mi vida, la etapa universitaria. La realización de este proyecto fin de carrera pone el broche final al camino iniciado hace unos años.

A mis padres, por su apoyo constante e incondicional. La educación que me han dado desde pequeña ha sido básica para ser lo que soy hoy en día.

A mi hermano Jaime, por estar siempre ahí, que aunque nos pasemos la mitad del tiempo enfadados, no podemos vivir el uno sin el otro.

A mi chico, por animarme, cuidarme y sacarme siempre una sonrisa, incluso en esos días en los que estoy insoportable.

A mis amigos de la universidad y amigas de la infancia, porque da igual el tiempo que pasemos sin vernos, sé que puedo confiar en vosotros en todo momento. Formáis parte de esa clase de familia que uno va eligiendo con el paso de los años y sin vosotros, nada sería lo mismo.

A mis compañeros de trabajo, por hacerme sentir uno más del grupo desde el primer día, ayudándome y enseñándome todo lo que sabéis, alentándome a dar lo mejor de mí cada día en la oficina. Siempre seréis mis chicos a pesar de que ya no trabajemos juntos.

Resumen

La telefonía móvil se ha convertido en una pieza fundamental en nuestras vidas, tanto a nivel profesional (dónde acceder a herramientas como el correo electrónico, datos corporativos o aplicaciones de negocio es esencial) como a nivel personal y de ocio (para comprar entradas de espectáculos o reservar mesa en un restaurante). Es la tecnología que más profundamente ha penetrado en nuestras vidas, haciéndonos cambiar incluso la forma en la que nos comunicamos o relacionamos.

No dudamos de llevar consigo el teléfono móvil cuando viajamos al extranjero y esperamos poder disfrutar de los mismos servicios que cuando nos encontramos en nuestro país de origen, pero ¿a qué precio? Muchos de nosotros hemos decidido apagar el teléfono móvil cuando nos encontrábamos en el extranjero por el miedo a la factura debido a los precios desorbitantes de las tarifas.

Los precios en itinerancia internacional o roaming han sido siempre excesivos debido a la escasa competencia entre las operadoras móviles a la hora de prestar servicios a los usuarios que se encontraban haciendo roaming en su red. La Unión Europea instó a las operadoras móviles a rebajar las tarifas y al no surtir efecto dicha recomendación, decidió regular el servicio de itinerancia internacional dentro de la Unión Europea, fijando unos precios máximos hasta la total abolición prevista para el año 2017.

Un gran porcentaje de los ingresos obtenidos en las operadoras móviles son generados por la itinerancia internacional. Las operadoras móviles deberán vigilar su negocio de roaming para continuar ofreciendo la mejor calidad de servicio a sus clientes en el extranjero reduciendo al máximo los costes generados por este servicio.

El objetivo principal de este proyecto fin de carrera es el estudio de los sistemas redirectores de tráfico de itinerancia internacional, que se convertirán en una herramienta clave para las operadoras, ya que serán capaces de redirigir a sus usuarios hacia aquellas redes en el país visitado que mayores ventajas les aporte, es decir, menor coste asociado y la mejor calidad de servicio posible. A través de casos de estudio y la descripción de todo el proceso de despliegue de la plataforma, comprenderemos cómo funcionan y si las expectativas desde el punto de vista técnico y de calidad de servicio se cumplen.

Abstract

Mobile telephony has become an essential part of our lives, both professionally (where the access to tools such as email, corporate data and business applications is a basic) as at personal and leisure level (buying tickets for shows or booking a table at a restaurant). The mobile technology that has deeply penetrated in our lives, making us even to change the way we communicate and interact each other.

No doubt to carry on the mobile phone when traveling abroad and hoping to enjoy the same services as when we are in our country, but at what price? Many of us have decided to turn the mobile phone off when we were abroad for fear of the invoice due to the exorbitant prices of the services tariff.

Prices for international roaming traffic were excessive due to the lack of competition between mobile operators when providing services to users who were roaming in their network. The European Union urged mobile operators to reduce the tariffs, but the recommendation did not take any effect, so it was decided to regulate international roaming service within the European Union, setting maximum prices until the total abolition scheduled for 2017.

A large percentage of the mobile operator's revenue is generated by the international roaming traffic. Mobile operators should monitor their roaming business to continue offering the best quality of service to their customers in foreign countries and minimising the costs generated by this service.

The main aim of this final project is the study of redirectors systems of international roaming traffic, which will become a key tool for operators, as they will be able to redirect their users to those networks in the visited countries that bring them the greatest benefits, I mean, lower associated costs and best quality of service possible. Through case studies and the platform deployment description process, we will understand how they work and if expectations from a technical and quality of service point of view are met.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción y objetivos

En Abril de 1973, Martin Cooper, director de Motorola presentó al mundo un artilugio que cambiaría nuestras vidas para siempre. Realizó la primera llamada telefónica desde un dispositivo móvil en la sexta avenida de Nueva York. Llamó a su máximo competidor, Joel Engel, jefe de desarrollo de la empresa AT&T y le dijo: “Joel, ¿a qué no sabes desde dónde llamo?”. Estas palabras supusieron el comienzo de una nueva era en el sector de las telecomunicaciones.

Desde entonces, el auge de las redes móviles ha sido imparable debido principalmente a la reducción del coste de los servicios y de los terminales, que han ido mejorando paulatinamente, consiguiendo mayor autonomía, pantallas de gran resolución y ofreciendo toda clase de servicios, no solamente voz como los primeros terminales móviles que salieron al mercado. Factores como la facilidad que ofrece la portabilidad para cambiarse de operadora, la cobertura en prácticamente cualquier lugar, la estandarización y la itinerancia internacional han sido básicos en su éxito a nivel universal.

Debemos mencionar también que la evolución de las distintas tecnologías que soportan la telefonía móvil sigue un ritmo imparable, en el que no da tiempo a desplegar una cuando ya se está considerando el despliegue de la siguiente.

La telefonía móvil y sus servicios asociados están muy presentes en nuestro día a día, hasta el punto en el que prácticamente no podemos separarnos de nuestros teléfonos móviles. Constantemente nos encontramos realizando llamadas, navegando por Internet, consultamos el correo electrónico, aplicaciones de mensajería instantánea, etc.

Sin embargo, existe aún una barrera que impide que la experiencia de usuario sea total y nos permita mantener nuestros hábitos y necesidades de estar conectados constantemente, independientemente de dónde nos encontremos, es decir, queremos seguir disfrutando de todos los servicios cuando viajamos a un país extranjero.

Los responsables son los altísimos precios que debemos pagar por utilizar nuestro teléfono móvil fuera de las fronteras del país dónde hemos contratado los servicios, lo que nos lleva normalmente a apagar el teléfono para evitar sorpresas en la factura.
Las políticas regulatorias europeas están poniendo freno a esta situación en los últimos años mediante el establecimiento de unos precios máximos imputables al abonado, anunciando la abolición total de estos costes para mediados del año 2017.

De esta regulación surge la necesidad de las operadoras móviles para vigilar su negocio de itinerancia internacional, ya que durante muchos años ha sido una de las mayores fuentes de ingreso para las operadoras.

Los sistemas redirectores de tráfico permitirán a las operadoras decidir la red que utilizarán sus abonados cuando se encuentren en el extranjero. Permitirá maximizar los beneficios a las operadoras, ya que se elegirán las redes con precios más competitivos. También se mejorará la calidad de los servicios ofrecidos permitiendo el uso de las redes con mejor cobertura o mejor infraestructura.

1.1 Objetivos

El principal objetivo de este proyecto fin de carrera es el estudio de los sistemas redirectores de tráfico de itinerancia internacional en las redes LTE, que es la tecnología que actualmente se está desplegando o está desplegada en las redes de las operadoras móviles. Dichos sistemas están enfocados a conseguir la mejor calidad de servicio posible minimizando los costes generados por el servicio de itinerancia internacional.

Los siguientes objetivos específicos se detallan a continuación:

- Descripción y entendimiento de la arquitectura de la red de acceso y red troncal específica de LTE, así como las principales funciones de sus entidades de red.

- Análisis del protocolo de señalización Diameter en el que se sustenta el interfaz de red objeto de estudio en este proyecto fin de carrera.

- Beneficios de la centralización del tráfico y la transición hacia los HUBs de itinerancia internacional por parte de las operadoras móviles.

- Estudio de los sistemas redirectores de tráfico:

    - Qué son y para que se utilizan.

- Mecanismos que utilizan para realizar la redirección del tráfico.
- Sus ventajas e inconvenientes.
- Entendimiento del funcionamiento primeramente en un entorno de laboratorio, para después ir a un entorno de tráfico real.

1.2 Fases del desarrollo

Especificamos a continuación cada una de las fases que han formado parte de este proyecto fin de carrera. Cada una de ellas ha sido básica y necesaria para una correcta comprensión e implementación de cada uno de los pasos dados.

- Familiarización con el entorno de trabajo: previamente a comenzar a trabajar, se debe producir un primer acercamiento al entorno en el que vamos a estar involucrados durante un período largo de tiempo. Herramientas de monitorización, traceo, sistemas de informes y alarmado serán piezas clave en este fase, así como empezar a configurar los DEAs del HUB de roaming.

- Estudio de las especificaciones de la 3GPP e ITU-T: continuando con el aprendizaje iniciado en la primera fase, seguiremos con las especificaciones técnicas sobre red LTE, itinerancia internacional y redirección de tráfico, así como la documentación distribuida por el proveedor del sistema redirector.

- Conexión directa HUB de roaming y migración de tráfico: durante las primeras semanas se trabajará en la implementación de la conexión directa para poder migrar el tráfico a posteriori. Éste será migrado en diferentes sub etapas, la primera de ella servirá para comprobar la correcta implementación de la conexión.

- Estudio casos previos a la redirección de tráfico: a lo largo de varias semanas se obtendrán datos sobre la distribución de los usuarios en las redes visitadas, datos que se utilizarán más tarde para hacer un estudio comparativo.

- Análisis de requisitos del sistema redirector: puesta en común de los requisitos que debería cumplir la plataforma para estudiar la viabilidad y los requerimientos necesarios para su implementación.

- Pruebas funcionales en entorno de laboratorio y producción: certificación de la funcionalidad del sistema redirector tanto en el entorno de laboratorio como en un escenario controlado con tráfico real.

- Migración tráfico a la plataforma de redirección y activación: fase muy parecida a la realizada durante la migración del tráfico de itinerancia internacional al HUB

de roaming. Estará subdividida en dos grandes fases para migrar el tráfico al redirector primero y después activar la redirección de forma secuencial.

- Estudio casos tras la redirección del tráfico: obtendremos datos de distribución de usuarios en las redes tras la aplicación de la redirección para los mismos casos estudiados con anterioridad, para que los datos sean consistentes a la hora de hacer la comparación de escenarios.

- Documentación: aunque desde el comienzo del proyecto se comenzó a documentar cada una de las tareas y funciones realizadas, es en la parte final cuando se trabaja más intensamente en la redacción de la memoria.

1.3 Medios empleados

Se dispondrá además de herramientas de monitorización y traceo para la verificación del tráfico en la red de producción. El proyecto describe el despliegue de un sistema de redirección de tráfico de itinerancia internacional en la red de un HUB de roaming.

Previa a la implantación de la plataforma en la red de producción o de tráfico real del HUB de roaming, contaremos con un entorno de laboratorio, que cuenta con un DEA de prueba y un simulador de tráfico para realizar un conjunto de pruebas que asegurarán el correcto funcionamiento del sistema. Éstas serán repetidas en el entorno de producción antes de la puesta en marcha de la plataforma para confirmar que los resultados y el funcionamiento es el esperado.

Se dispondrá además de herramientas de monitorización y traceo para la verificación del tráfico en la red de producción.

1.4 Estructura de la memoria

Este proyecto fin de carrera ha sido estructurado en seis capítulos y un anexo, los cuales serán descritos brevemente a continuación:

- Capítulo 1. Introducción. Se trata de una breve introducción al proyecto, incluyendo los objetivos y motivaciones que provocaron la aparición de los sistemas redirectores de tráfico internacional. Se describirán además las distintas fases de desarrollo y los medios utilizados en la realización del proyecto.

- Capítulo 2. Redes LTE. Basándonos en la arquitectura genérica de los sistemas celulares 3GPP, se hará una descripción pormenorizada de cada entidad de red, los interfaces que las interconectan y el protocolo de señalización utilizado en estas redes.

- Capítulo 3. Itinerancia Internacional. Descripción del servicio y de la arquitectura de las redes LTE cuando deben proveer dicho servicio.

- Capítulo 4. Centro de gestión de itinerancia internacional. Objetivo y requisitos que deben cumplir los centros gestores de itinerancia, así como las posibles implementaciones que se pueden realizar.

- Capítulo 5: Redirección del tráfico de itinerancia internacional. Descripción del funcionamiento básico y los mecanismos utilizados por estos sistemas para realizar la redirección del tráfico de itinerancia internacional.

- Capítulo 6: Análisis y estudio del sistema redirector de tráfico. Muestra el proceso llevado a cabo para el despliegue del sistema de redirección en una red comercial, analizando diferentes casos de estudio que mostrarán la efectividad de dicho sistema.

- Capítulo 7: Conclusiones y líneas futuras. Posibles líneas futuras de trabajo basadas en las conclusiones obtenidas del proyecto o de la situación que vive el sector de la telefonía móvil.

- Anexo A: Planificación y presupuesto. Contiene los plazos de realización y los costes asociados al proyecto fin de carrera.

Capítulo 2

Redes LTE

En este capítulo inicial comenzaremos a describir los conceptos básicos que serán necesarios para la clara comprensión de este proyecto fin de carrera. Describiremos la arquitectura de una red de comunicaciones móviles basada en las especificaciones del sistema LTE. Para ello, partiremos de un estudio inicial de la arquitectura genérica de los sistemas 3GPP, identificando las piezas clave que componen la arquitectura de red. Este análisis nos permitirá ver de forma clara cuales son los nuevos componentes introducidos por el sistema LTE respecto a las redes GSM y UMTS.

Una vez identificados los componentes que forman parte del sistema LTE, realizaremos una descripción detallada de cada uno de ellos, indicando las funciones de las entidades de red, los interfaces asociados y protocolos utilizados. En la última sección se hablará del procedimiento de traspaso al dominio de circuitos (CSFB, Circuit Switched Fallback), ya que las redes LTE actuales siguen utilizando el dominio de circuitos para el encaminamiento del tráfico de voz.

2.1 Nacimiento de las tecnologías 4G

La evolución de la telefonía móvil, como hemos repasado en el capítulo de introducción, ha pasado por distintas generaciones, denominadas 1G, 2G y 3G, siendo la primera de ellas analógica y las siguientes, digitales [1]. Ahora nos encontramos en fase de introducir los sistemas pertenecientes a la cuarta generación, también digital, los cuales presentan

bastantes diferencias con las generaciones anteriores en cuanto a la infraestructura de la red, que utiliza el protocolo de Internet (IP) como base, pero, sobre todo, en cuanto a capacidad de transferencia de datos.

Generalmente se suele hablar de los sistemas 4G para referirse a todos los sistemas sucesores de los de 3G y 3.5G, sin embargo existe cierta confusión y a algunas veces se asignan tecnologías a generaciones de una manera que no es del todo correcta. Siendo estrictos LTE (Long Term Evolution) no es un sistema de la cuarta generación ya que debemos hacer distinción entre los sistemas 3.9G y 4G porque existen algunas diferencias destacables entre ellos. Sin embargo, admitiremos como cuarta generación a los sistemas actuales de 3.9G pues suponen un avance importante con respecto a la generación anterior en cuestiones de prestaciones y capacidad.

La división de radiocomunicaciones de la Unión Internacional de las Telecomunicaciones (ITU-R, International Telecommunication Union – Radio communication) publicó en el año 2008 un documento conocido como 4G o IMT (International Mobile Telecommunications) Avanzado estableciendo los requerimientos básicos para los servicios de cuarta generación. En este documento se dice que la cuarta generación deberá ser una red completamente nueva, una red de redes y un sistema de sistemas integrados, basado enteramente en la conmutación de paquetes con el protocolo IP, compatible tanto con la versión 4 como 6. Las redes serán capaces de proporcionar velocidades de datos de bajada de 100Mbit/s y hasta un 1Gbit/s en subida de datos. Las redes tendrán calidad de servicio y alta seguridad extremos a extremo, ofreciendo cualquier tipo de servicio en cualquier momento y en cualquier lugar, con interoperabilidad entre sí. El documento IMT Avanzado suponía la evolución del documento IMT-2000 que cubría las tecnologías relativas a 3G, 3.5G y 3.75G.

Las tecnologías candidatas a 3.9G, pues no cumplían con todos los requerimientos definidos por el IMT avanzado, son (aunque en el año 2010 fueron reconocidas como tecnologías LTE por la ITU-R):

- **LTE** (Long Term Evolution): LTE es la tecnología definida por el 3GPP donde participan los principales operadores y fabricantes para definir los estándares. Es en la release 8 de sus especificaciones, cuando 3GPP completó el que es su sistema LTE, cuyo principal objetivo es proporcionar un acceso radio de alto rendimiento, que permita altas velocidades de transmisión y recepción en dispositivos móviles y que pueda coexistir con sistemas anteriores, permitiendo a los operadores una rápida y sencilla migración hacia esta nueva tecnología. Sin embargo, tampoco cumplió con los requerimientos básicos especificados por el IMT Avanzando, pues la velocidad de datos de bajada era de 100 Mbit/seg y la de subida de 50 Mbit/seg. La operadora Telia Sonera fue la pionera en el despliegue de dicha tecnología en Suecia y Noruega.

- **Mobile WiMAX** (Worldwide Interoperability for Microwave Access) **802.16e**: WiMAX es un sistema de comunicación digital inalámbrico definido en el estándar del IEEE 802.16 para redes de área metropolitana que provee comunicaciones de banda ancha con cobertura amplia. Es una tecnología que no ha sido utilizada en Europa cuyas velocidades de datos de bajada eran de 128 Mbit/seg y56 Mbit/seg para la subida. La primera implementación se realizó en el

año 2006 por parte de la operadora KT de Corea del Sur y la operadora Sprint de Estados Unidos en el año 2008.

En el año 2010, se completó la evaluación de las 6 nuevas propuestas candidatas a la tecnología 4G. De entre todas ellas, dos tecnologías, LTE-Advanced y WiMAX 802.16m o WiMAX2 cumplieron con todos los criterios establecidos en el documento IMT avanzado, por lo que se las designó como tecnología 4G de manera oficial. Nacía así oficialmente la nueva generación mundial de tecnologías móviles. Veamos cada una ellas:

- **LTE-Advanced**: en la release 10 es cuando se inicia la especificación, pero no se trata de una nueva tecnología, sino de una mejora de la ya existente y definida en la release 8. La velocidad de datos de bajada aumentó hasta los 3Gbit/seg y a 1.5Gbit/seg para la subida. La operadora rusa Yota fue la primera en desplegar LTE-Advanced en su red seguida en el año 2013 por la operadora Verizon de Estados Unidos.

- **Mobile WiMAX release 2 802.16m**: el estándar 802.16m o WiMAX móvil consigue al fin en esta especificación cumplir con las velocidades especificadas en el documento IMT avanzado.

En la siguiente tabla podemos apreciar las diferentes velocidades de datos para las tecnologías englobadas dentro de la cuarta generación.

	IMT-Advanced	LTE	802.16e MovileWiMAX	LTE-Advanced	802.16m Mobile WiMAX2
Velocidad descarga máxima	1Gbit/seg	100Mbit/seg	128Mbit/seg	3Gbit/seg	1Gbit/seg
Velocidad subida máxima	100Mbit/seg	50Mbit/seg	56Mbit/seg	1.5Gbit/seg	100Mbit/seg

Tabla 1: Velocidad datos de las tecnologías 4G

Desde hace muchos años, el tener un único sistema global de telecomunicaciones que permita al usuario utilizar los servicios en cualquier parte del mundo ha sido uno de los grandes objetivos de la industria de las telecomunicaciones. En la segunda generación, liderada por la tecnología GSM, quedaba la fragmentación con CDMA, TDMA e IDEN. Con el paso a 3G, casi todos los operadores TDMA migraron a la tecnología 3GPP, sin embargo continuaba la división histórica entre GSM y CDMA.

Ahora con LTE, parece lograrse ese objetivo de tener una tecnología global estándar. La mayoría de los operadores líderes, fabricantes de dispositivos e infraestructura dan soporte a LTE como la tecnología móvil global.

2.2 Arquitectura de red LTE

Las arquitecturas de red de la familia de sistemas especificados por 3GPP se adaptan a la arquitectura mostrada en la Figura 1. Los sistemas 3GPP abarcan la especificación del equipo de usuario y de una infraestructura de red dividida de forma lógica en una infraestructura de red de acceso y una de red troncal [2].

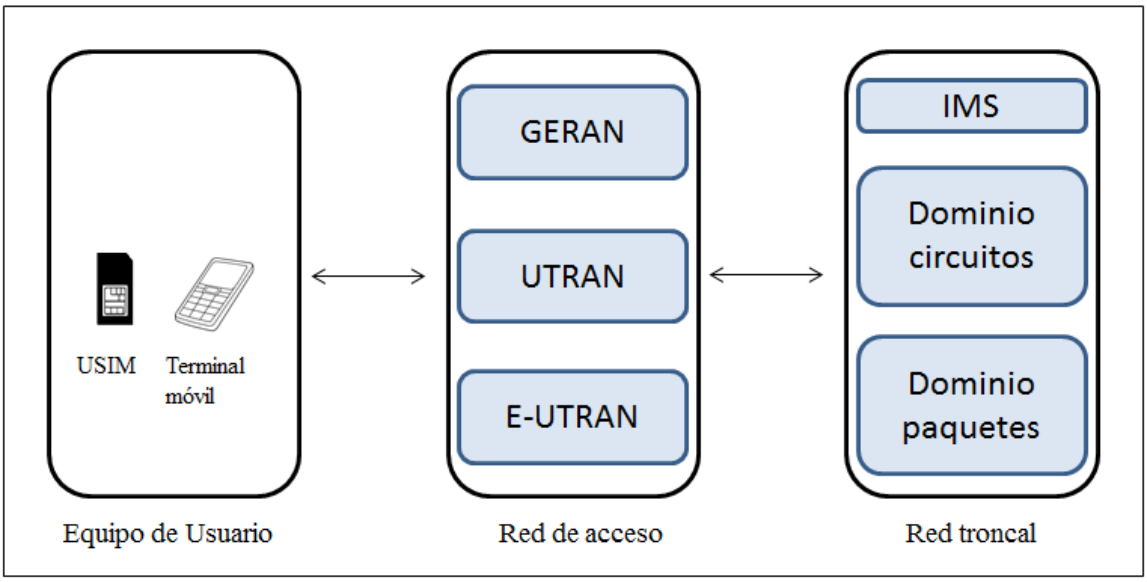

Figura 1: Arquitectura a alto nivel de los sistemas 3GPP

El equipo de usuario es el dispositivo que permite al usuario acceder a los servicios ofrecidos por la red. Se compone de dos elementos básicos: el dispositivo móvil o terminal y una tarjeta inteligente, UICC (Universal Integrated Circuit Card). La tarjeta UICC es también conocida como SIM (Subscriber Identity Module) en los sistemas GSM y USIM (Universal Subscriber Module) en los sistemas UMTS y LTE. Es la encargada de almacenar la información y sustentar los procedimientos relacionados con la subscripción del usuario a los servicios proporcionados por la red.

Respecto a la red de acceso, es la parte del sistema responsable de mantener la transmisión radio con los equipos de usuario con el fin de proporcionar la conectividad necesaria entre éstos y los equipos de la red troncal.
Está compuesta por estaciones base y por equipos controladores de estaciones base. 3GPP ha especificado tres tipos de redes de acceso diferentes:

- GERAN (GSM EDGE Radio Access Network).
- UTRAN (UMTS Terrestrial Radio Access Network).
- E-UTRAN (Evolved UTRAN). Ésta última, es la nueva red de acceso para los sistemas LTE.

La red troncal es la encargada de funciones tales como el control de acceso a la red celular, la gestión de la movilidad de los usuarios, la interconexión con otras redes, la gestión de las sesiones de datos y está dividida de forma lógica en:

- Dominio de circuitos, engloba todas las entidades de la red troncal que participan en la provisión de servicios de telecomunicación basados en conmutación de circuitos, es decir, servicios a los que se les asignan recursos de forma dedicada, circuitos, en el momento del establecimiento de la conexión, manteniéndose hasta la finalización del servicio. El dominio de circuitos es sólo accesible a través de las redes de acceso GERAN y UTRAN.

- Dominio de paquetes, incluye todas las entidades de la red troncal que proporcionan servicios de telecomunicación basado en la conmutación de paquetes. La información de usuario se estructura en paquetes de datos que se encaminan y transmiten por los diferentes elementos y enlaces de red. Existen dos implementaciones diferentes del dominio paquetes: GPRS, es la implementación desarrollada para las redes GSM y UMTS, y EPC, es la nueva especificación creada para los sistemas LTE.

- Subsistema IP Multimedia (IMS IP Multimedia Subsystem), comprende los elementos relacionados con la provisión de servicios IP Multimedia basado en el protocolo SIP (Session Initiation Protocol). Esta parte de la red troncal es responsable de la señalización asociada a los servicios multimedia y utiliza como mecanismo de transporte los servicios de transferencia de datos proporcionados por el dominio de paquetes.

Teniendo en mente la arquitectura genérica de los sistemas 3GPP, vamos ahora a centrarnos en la arquitectura de un sistema LTE, al que se denomina formalmente en las especificaciones como Evolved Packet System (EPS).

Los componentes fundamentales del sistema LTE son la nueva red de acceso E-UTRAN (Evolved-UMTS Terrestrial Radio Access Network) y el nuevo dominio de paquetes EPC (Evolved Packet Core) de la red troncal. Los diferentes elementos han sido diseñados para soportar todo tipo de servicios de telecomunicación mediante mecanismos de conmutación de paquetes, por lo que no es necesario disponer de un componente adicional para la provisión de servicios en modo circuito.

La red de acceso E-UTRAN y la red troncal EPC proporcionan de forma conjunta servicios de transferencia de paquetes IP entre los equipos de usuario y redes de paquetes externas tales como IMS y/o otras redes de telecomunicaciones como Internet.

Otra característica de LTE es que se contempla también el acceso a sus servicios a través de GERAN y UMTS, así como a través de otras redes de acceso que no pertenecen a la familia 3GPP como son CDMA2000, Mobile WiMAX, redes 802.11..., para ello, se han definido una serie de interfaces en el EPC para la interconexión de diferentes redes de acceso.

2.2.1 Red de acceso: E-UTRAN

En la red de acceso E-UTRAN la única entidad de red que encontramos es la estación base, que en esta generación es denominada *Evolved NodeB* (eNB) [3]. Integra todas las funcionalidades de la red de acceso, lo que supone un cambio con respecto a las generaciones anteriores, ya que en éstas, a parte de las estaciones base (BTS para GSM y NodeB para UMTS), existe un equipo controlador (BSC para GSM y RNC para UMTS).

Un aspecto clave del eNB es la gestión de los recursos radio, pues todos los protocolos específicos de la interfaz radio acaban en él. Mediante dichos protocolos, el eNB realiza la asignación de los recursos radio para la transmisión ordenada de paquetes y controla la movilidad de los usuarios cuando tienen que cambiar de eNB que les de servicio (traspaso de eNB). También se encarga de la selección dinámica de la entidad MME (Mobility Management Entity) de la red troncal EPC cuando un usuario se registra en la red, pudiendo estar conectado de forma simultánea a un conjunto de MMEs (pool area).

El eNB también puede interactuar con otro nodo de la red troncal EPC, el S-GW (Serving Gateway) que le sirve de pasarela para el encaminamiento de tráfico a los usuarios, pero en este caso, el eNB no puede seleccionar el S-GW correspondiente.

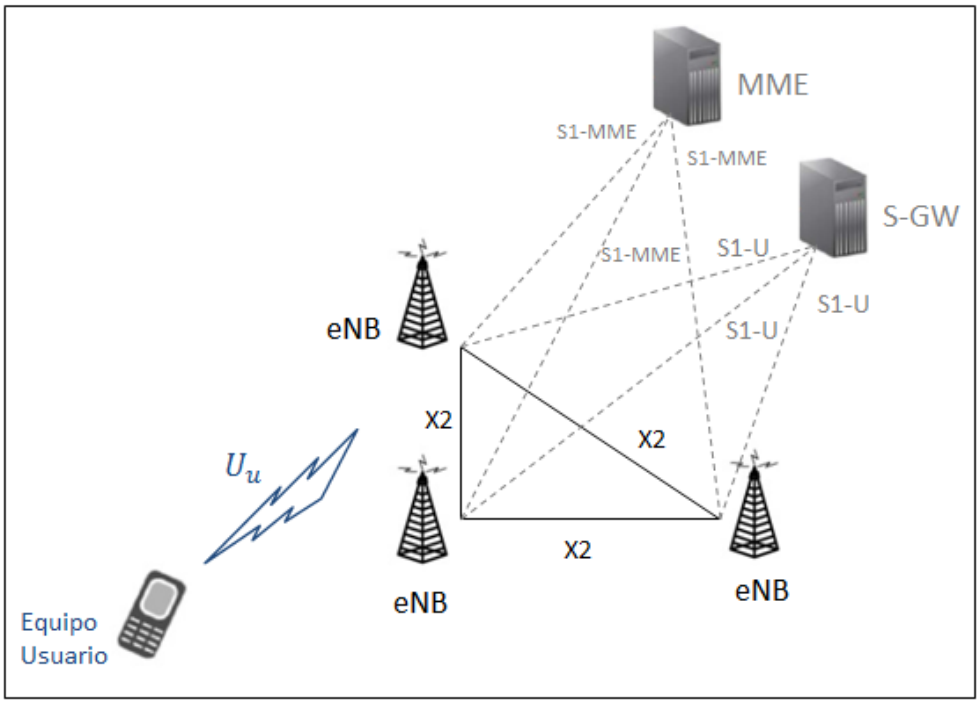

Figura 2: Red de acceso E-UTRAN

Como podemos observar en la figura 2, el eNB tiene interfaces para comunicarse con otros eNB, con los equipos de usuario y con la red troncal EPC.

- Interfaz S1: es el interfaz que conecta el eNB con la red troncal EPC y está a su vez dividida en dos:

- S1-MME: conecta el eNB con el MME, sustentando las funciones y procedimientos necesarios para la gestión del interfaz y del eNB.
- S1-U: conecta el eNB con el S-GW para la transferencia de datos de usuario. No hay garantía de entrega pues está basado en el protocolo UDP (User Datagram Protocol) ni soporta mecanismos de control de errores ni control de flujo.

- Interfaz X2: interfaz que utilizan los eNB para comunicarse entre sí y por donde intercambian mensajes de señalización para realizar una gestión eficiente de los recursos radio, además de transferir el tráfico de los usuarios cuando estos se desplazan a otro eNB.

- Interfaz E-UTRAN U_u: también conocido como interfaz LTE U_u o simplemente interfaz radio LTE, permite la transferencia de información por el canal radio entre el eNB y los equipos de usuario.

2.2.2 Red troncal: EPC

La finalidad básica de esta nueva arquitectura es proporcionar conectividad IP para todos los servicios. Además, el diseño de la red troncal hace posible acceder a los servicios a través de cualquier red de acceso 3GPP como GERAN o UTRAN e incluso de las que no pertenecen a la familia 3GPP.

En la red troncal EPC se realiza una separación entre el plano de usuario y el plano de control:

- Plano de usuario: es el tráfico de datos transmitido entre dos usuarios independientemente de su naturaleza.

- Plano de control: tráfico relativo a los protocolos de señalización que permiten a los diferentes componentes de la red troncal EPC inter-operar para poder ofrecer servicios de transmisión que datos a los clientes.

Nosotros nos centraremos en el estudio de la red trocal EPC cuando la red de acceso es 3GPP, tal y como se recoge en la especificación 3GPP TS 23.401 [4].

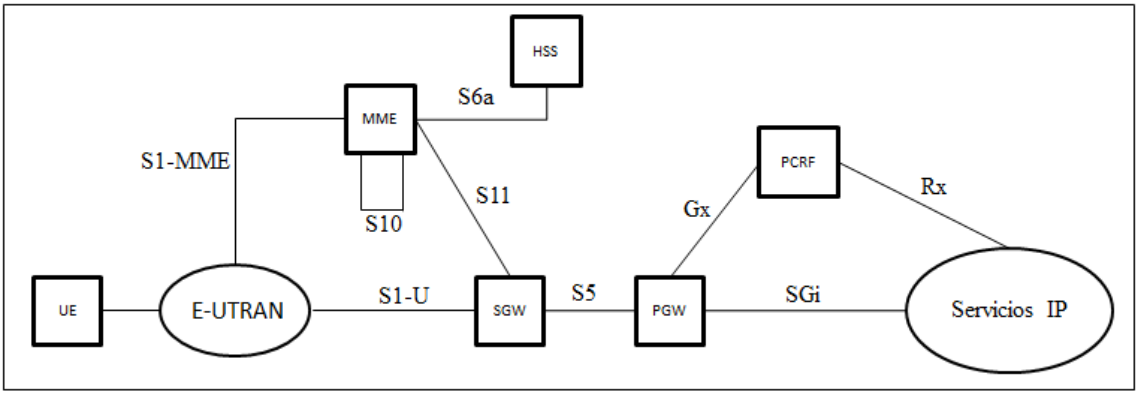

Figura 3: Red troncal EPC

El núcleo de la red troncal EPC está formado por tres entidades de red, MME (Mobility Management Entity), Serving Gateway (S-GW) y el Packet Data Network Gateway (P-GW), que junto con la base de datos principal del sistema denominada HSS (Home Subscriber Server), constituyen los elementos principales para la prestación del servicio de conectividad IP entre los equipos de usuario conectados al sistema a través de la red de acceso E-UTRAN y las redes externas a las que se conecta la red troncal EPC.

Definimos a continuación cada una de las entidades de red mencionadas:

- **MME**: es el elemento principal del plano de control que gestiona el acceso de los usuarios a través de la red de acceso E-UTRAN. Todo terminal que se encuentre registrado en la red y sea accesible a través de E-UTRAN, tiene un MME asignado. Sus funciones principales son:

    - Autenticación y autorización del acceso de los usuarios siempre a través de E-UTRAN.
    - Gestión de la señalización que se necesita establecer, mantener, modificar y liberar de los servicios portadores.
    - Gestión de la movilidad de los usuarios cuyo terminal no tiene una conexión establecida con la red de acceso pero están dentro del área de servicio de la red.
    - Señalización para el soporte de movilidad entre EPS y otras redes externas.

    Supone la evolución de las funciones realizadas por la BSC y MSC

- **SGW** (Serving Gateway): es la pasarela para el tráfico de usuario entre la red de acceso y la red troncal. Todo usuario registrado tiene asignado una entidad S-GW a través de la cual transcurre su plano de usuario. Las principales características son:

    - Proporciona un punto de anclaje en la red troncal con respecto a la movilidad del terminal entre eNBs.
    - Proporcional un punto de anclaje también para la gestión de la movilidad con otras redes de acceso 3GPP.

- Encaminamiento del tráfico de usuario. Alberga la información y funciones necesarias en encaminamiento necesarias para dirigir el tráfico hacia la pasarela P-GW o el eNB que corresponda.

- **PDN Gateway** (P-GW, Packet Data Network Gateway): entidad encargada de proporcionar la conectividad entre la red LTE y las redes externas ya que sirve de pasarela entre ambas. Los usuarios tienen asignada al menos una pasarela P-GW desde su registro en la red.

    - Actúan como punto de anclaje para la gestión de movilidad entre LTE y redes externas no 3GPP.
    - Asignación de direcciones IP a los usuarios para ser utilizadas en redes externas.
    - Aplicación de reglas de uso de la red y control de tarificación para los servicios que tenga establecidos el terminal.

- **HSS** (Home Subscriber Server): es la base de datos principal que almacena la información de los usuarios en red. No solo contiene información relativa a la subscripción del usuario, sino también información con respecto a la operativa de la red. Entre la información que almacena, cabe destacar los identificadores universales de usuario (IMSI, International Mobility Subscriber Identity), identificadores de servicio, información de seguridad y cifrado o la información de localización del usuario en la red.

  El HSS supone la fusión del HLR (Home Location Register) y el AuC (Authentication Center), dos entidades utilizadas en las redes GSM.

No podemos olvidarnos de la entidad PCRF (Policy and Charging Rules Function) que forma parte del sistema PCC (Policy and Charging Control) que se utiliza para controlar los servicios ofrecidos por la red, así como para controlar los mecanismos de tarificación.

2.2.2.1 Interfaces

A continuación describimos brevemente cada uno de los interfaces que aparecen en la figura 3, deteniéndonos más en el interfaz S6a, ya que soporta escenarios de itinerancia internacional donde el MME de una operadora, puede acceder al HSS de otra operadora. Es el interfaz en el que se sustenta este proyecto fin de carrera.

- Interfaz SGi: interconecta la pasarela P-GW de la red LTE con las redes externas, pudiendo ser una red privada o pública. Desde la perspectiva de la red externa, la pasarela P-GW es vista como un router IP convencional.

- Interfaz S5: soporta la transferencia de paquetes de usuario entre las pasarelas P-GW y S-GW cuando ambas pasarelas se encuentran en la misma red.

- Interfaz S8: es idéntico al interfaz S5 pero en escenarios de itinerancia internacional, es decir, cuando la pasarela S-GW pertenece a la red visitada y la pasarela P-GW a la red local del usuario.

- Interfaz S11: interconecta al MME con la pasarela S-GW lo que supone el nexo de unión entre el plano de control (entre MME y terminal de usuario) y el plano de usuario de la red troncal.

- Interfaz S10: está definido entre dos MMEs y su principal función es el soporte al mecanismo de reubicación de la entidad MME.

- Interfaz Rx: permite conectar el PCRF a otras redes de operadores de servicios IP.

- Interfaz S7: soporta la transferencia de políticas de calidad de servicio y reglas de cobro desde el PCRF al P-GW.

- Interfaz S6a: permite la transferencia de información entre la base de datos HSS y el MME, dando soporte a las siguientes funciones:

    - Mantenimiento de información de gestión de la localización. El HSS almacena la identificación del MME que controla a cada usuario registrado en la red. Cuando el terminal se conecta a un nuevo MME, éste puede recuperar la información relativa al MME que previamente le dio servicio para realizar la reubicación pertinente.
    - Autorización de acceso a la red LTE. El HSS almacena los datos de subscripción de los usuarios que condicionan el acceso a los servicios que ofrece la red. Estos datos son transferidos al MME que ejecutará una serie de comprobaciones para autorizar o no el uso de un determinado servicio.
    - Autenticación de los usuarios. A través de dicho interfaz, el MME se descarga la información que permite llevar a cabo el procedimiento de autenticación del usuario.
    - Notificación y descarga de la identidad de la pasarela P-GW que utiliza el usuario en una conexión. El HSS almacena la información relativa a las pasarelas P-GW que dan servicio al usuario para poder dar soporte en los mecanismos de movilidad entre LTE y otras redes no 3GPP.

La interfaz S6a se basa en el protocolo de señalización Diameter y que será descrito en la siguiente sección del capítulo.

2.2.2.2 Protocolo Diameter

El protocolo Diameter es una evolución del protocolo RADIUS, inicialmente diseñado para dar soporte a las funciones de autorización, autenticación y accounting (AAA, Authorization Authentication Accounting) para las aplicaciones que involucran el acceso a redes o a aplicaciones IP. Mejora las prestaciones de su predecesor en aspectos tales como seguridad, robustez frente a pérdidas de mensajes, así como su extensibilidad que permite el uso del protocolo para las aplicaciones fuera del ámbito AAA.

El protocolo Diameter se estructura en torno al protocolo Diameter base, definido en el RFC 3588 “Diameter Base Protocol” [5] y a un número de extensiones denominadas aplicaciones Diameter. El protocolo base define los aspectos fundamentales del protocolo Diameter: formato de los mensajes y elementos de información genéricos

(AVPs, Attribute Value Pairs), mecanismos de transferencia de mensajes, descubrimiento de capacidades de las entidades Diameter y aspectos de seguridad.

Las aplicaciones Diameter definen los mensajes adicionales y los procedimientos necesarios para adaptar el uso de Diameter al soporte de una determinada funcionalidad. Entre las aplicaciones de Diameter más relevantes estandarizadas por IETF se encuentran: la aplicación NAS (Network Access Server) de la RFC 4005, la aplicación de diameter para servicios AAA en el marco de control de acceso a redes.

A nosotros la aplicación que nos interesa en el ámbito de este proyecto fin de carrera, es la aplicación S6a para la gestión de la movilidad de los usuarios en la red troncal EPC y especificada por la 3GPP en la norma TS 29272.

Las siguientes definiciones básicas nos ayudarán a una mejor comprensión del protocolo:

- Aplicación Diameter: cada interfaz de red que utiliza el protocolo Diameter, es una aplicación Diameter pues amplía las capacidades del protocolo base. La interfaz S6a, A9, Gx son aplicaciones Diameter.

- Comandos: son los mensajes que forman parte de la aplicación. Cada comando tiene dos mensajes, uno de solicitud o petición y otro de respuesta.

- AVP: forma ordenada de representar los parámetros que caracterizan los mensajes de solicitud/petición y respuesta.

El protocolo Diameter es un protocolo peer-to-peer, cualquiera de los compañeros puede mandar una petición al otro compañero y está basado en el concepto de cliente/servidor:

- Un **servidor** Diameter no es el nodo que manda la respuesta a una petición, sino, que autentifica y autoriza la petición recibida. En la aplicación S6a, el nodo que actúa como servidor Diameter es el HSS.

- Un **cliente** Diameter no está referido al nodo que manda las peticiones, sino que es un nodo que se encarga de controlar el acceso a la red. En la aplicación S6a, el nodo que actúa como cliente Diameter es el MME.

Todos los mensajes Diameter son peticiones o respuestas y para poder intercambiarlos, tanto cliente como servidor deben tener implementado el protocolo Diameter base y la misma aplicación.

A parte de la distinción entre servidor y cliente, los agentes Diameter pueden clasificarse en:

- Agent **relay**: son agentes que aceptan y enrutan mensajes de otros nodos hacia su destino, en función de la información de enrutamiento contenida en el mensaje y de las tablas de enrutamiento Diameter basadas en el realm. Nunca originan mensajes y sólo analizan la parte relativa al enrutamiento. Modifica el mensaje ya que puede borrar o añadir información relativa al enrutamiento exclusivamente.

- Agentes **proxy**: aparte de realizar las funciones de los agentes relay, toman decisiones en base a las políticas de acceso y uso de recursos que tenga definidas. Su funcionalidad depende de la aplicación, así que necesita conocer la semántica de los mensajes Diameter. Puede modificar y rechazar mensajes en función de las políticas definidas.

- Agente **redirect**: son agentes que tan sólo re direccionan el mensaje hacia el destino sin alterar el mensaje.

- Agente **translate**: realiza la traducción entre dos protocolos, como por ejemplo entre RADIUS y Diameter o MAP y Diameter.

Otro concepto que debemos tener en mente:

- **Conexión**: se realiza a nivel de transporte y se establece entre dos entidades iguales para enviar y recibir mensajes Diameter.

- **Sesión**: no se trata de una conexión, es un concepto que se establece a nivel de la capa de aplicación entre un cliente y un servidor.

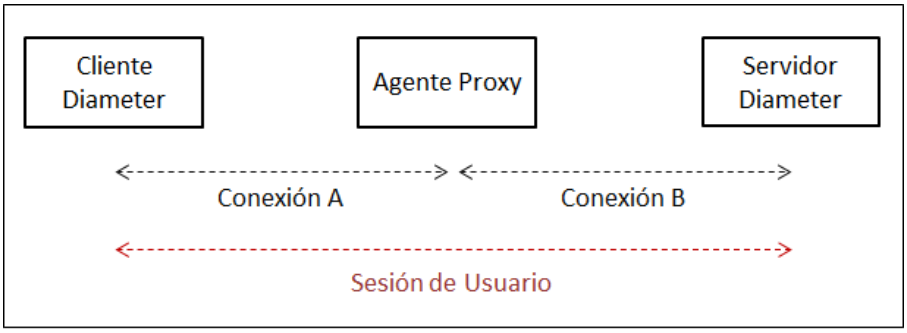

Figura 4: Concepto de sesión y conexión en Diameter

Formato de los mensajes Diameter

La cabecera de los mensajes tiene el siguiente formato:

Diameter Header																															
Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	version								message length																							
32	R	P	E	T					command code																							
64	application ID																															
96	hop-by-hop ID																															
128	end-to-end ID																															
160	AVPs																															
...	...																															

Figura 5: Cabecera mensaje Diameter

- Version: el campo versión siempre debe estar a 1 para indicar que la versión de Diameter es 1.

- Message length: campo que indica el tamaño del mensaje incluyendo la cabecera.

- Command flags: dan información sobre el mensaje:

    - R (request), si el bit está a 1, el mensaje es una petición. Si está a 0, es una respuesta.
    - P (proxiable): si el bit está a 1, el mensaje puede ser reenviado o redirigido. Si está a 0, se tratará de forma local.
    - E (error): si el bit está a 1, el mensaje contiene un error.
    - T (potentially re-transmitted): si el bit está a 1, es un mensaje que ha sido retransmitido después de haberse producido un fallo en el link de enrutamiento.

- Command-code: código que identifica el tipo de mensaje relativo a la aplicación. En la siguiente tabla mostramos los Command-code el protocolo base.

Nombre del comando	Abreviatura	Código
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchange-Request	CER	257
Capabilities-Exchange-Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275

Tabla 2: Códigos de comando Diameter Base

- Application-ID: identifica la aplicación a la que pertenecen los mensajes. El identificador para la aplicación S6a es 16777251.

- Hop-by-Hop ID: campo de la cabecera utilizado para emparejar las peticiones con las respuestas.

- End-to-end ID: se utiliza para identificar mensajes duplicados. Este campo no puede ser modificado por ningún agente.

Y el formato de los AVPs:

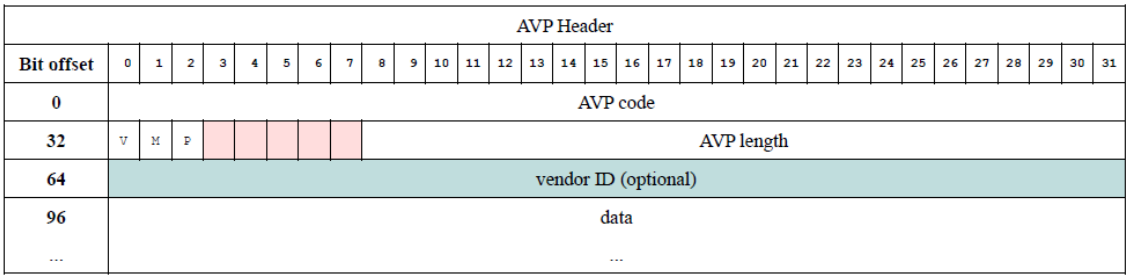

Figura 6: Formato AVPs Diameter

- AVP Code: este parámetro combinado con el vendor ID identifican de forma inequívoca al atributo.

- AVP Flags: informan al receptor de cómo debe tratar el AVP.

    - V (Vendor Specific bit): indica si el campo opcional de identificación del proveedor (vendor-ID) está presente en el mensaje.
    - M (Mandatory bit): si el bit está a 1, el mensaje no debe ser rechazado aun siendo desconocido el AVP.
    - P (Protected bit): si el bit está a 1, indica que se necesita encriptación para la seguridad extremo a extremo del mensaje.

- AVP length: indica la longitud del AVP sin contar con la cabecera.

- Vendor-ID: si el AVP ha sido creado por algún proveedor en concreto, en este campo se especificará cual es. Los AVPs definidos para la aplicación S6a han sido creados por el 3GPP cuyo Vendor-ID es 10415.

El protocolo Diameter base aunque tiene una lista de 49 AVPs, nosotros solo vamos a mencionar aquellos que nos serán útiles para enrutar mensajes:

- Origin-Host AVP: debe estar presente en todos los mensajes e identifica a la identidad que ha originado el mensaje.

- Origin-realm AVP: contiene el realm o dominio de la entidad que ha originado el mensaje y está siempre presente en todos los mensajes.

- Destination-Host AVP: nunca se encuentra en las respuestas y no siempre está presente en las peticiones. Identifica a la identidad a la que se le quiere enviar el mensaje.

- Destination-realm AVP: contiene el realm o dominio de la entidad a la que se le quiere enviar el mensaje y solo está presente en las peticiones, no en las respuestas.

- User-Name AVP: es el IMSI de la operadora cuando la aplicación es S6a.

- Session-ID: identifica la sesión de usuario, todos los mensajes de la sesión tendrán el mismo identificador.

- Result-Code AVP: indica si una petición ha sido completada satisfactoriamente o ha ocurrido un error. Todos los mensajes de respuesta contienen este AVP. Tenemos los siguientes códigos de resultado:

    - 1XX: informan al que ha enviado la petición de que será errónea si sigue adelante.
    - 2XX: informan del éxito del mensaje.
    - 3XX: informan de errores de protocolo.
    - 4XX: informan de fallos temporales.
    - 5XX: informan de fallos permanentes.

- Experimental-Result-Code AVP: es un AVP que agrupa el Vendor-ID AVP con el Result-Code AVP informando si la petición ha sido completada satisfactoriamente o ha ocurrido un error.

Vamos a describir ahora como los nodos Diameter establecen la conexión entre ellos y como se comunican. En la figura 7, se describe el flujo de mensajes desde que se inicia la conexión hasta que uno de ellos decide terminarla.

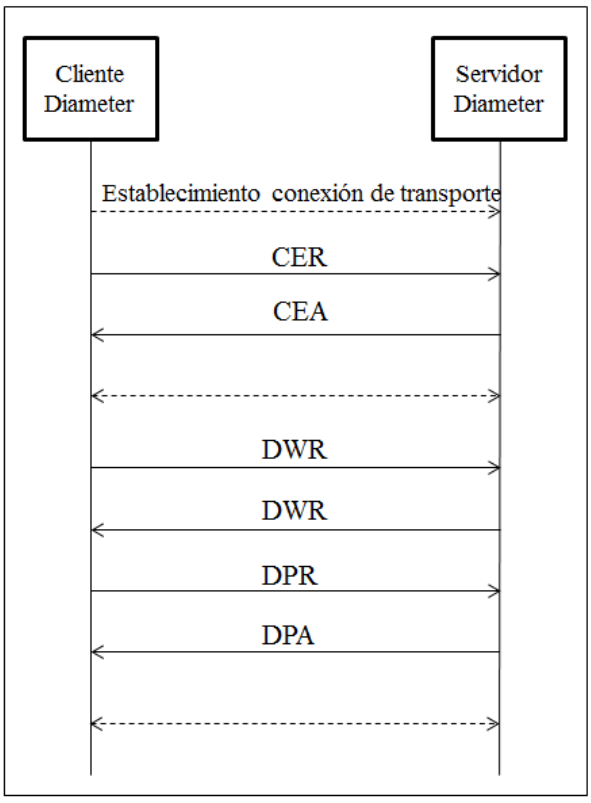

Figura 7: Establecimiento conexión Diameter

Una vez se ha establecido la conexión de transporte, los dos nodos Diameter deben intercambiar mensajes para conocer la identidad y aplicaciones del otro. Lo hacen a través de los códigos de comando CER (Capabilities-Exchange-Request) y CEA (Capabilities-Exchange-Answer). Los nodos Diameter deben almacenar las aplicaciones que el otro nodo maneja para evitar enviarle AVPs que no son propios de esa aplicación.
El nodo Diameter que recibe el CER, comprueba las aplicaciones y si al menos una coincide con las suyas, contesta con un CEA informando al nodo Diameter de las aplicaciones que es capaz de manejar.

Sin embargo, si el nodo Diameter que recibe el CER no tiene ninguna aplicación en común con el nodo originante o es desconocido para él, contestará con un CEA y un código de resultado asociado además de dar por finalizada la conexión de transporte.
Una vez los comandos CER/CEA se han completado satisfactoriamente, la conexión está preparada para los mensajes propios de la aplicación o aplicaciones que tengan en común. Nosotros, esperaríamos ver mensajes de la aplicación S6a, pues es el interfaz bajo estudio en este proyecto. En el próximo capítulo, en la sección de enrutamiento, explicaremos como se realiza el routing de los mensajes Diameter de la aplicación S6a.

Cuando no se están enviando mensajes relativos a ninguna aplicación en la conexión, uno de los agentes puede enviar mensajes al otro para comprobar que la conexión sigue establecida. Son los comandos que aparecen en la figura como DWR (Device Watchdog Request) y DWA (Device Watchdog Answer) y sirven como mecanismo para detectar fallos de conexión a nivel de transporte de forma pro activa.

Por último, cualquiera de los agentes Diameter puede dar por finalizada la conexión mediante los comandos DPR (Disconnect Peer Request) y DPA (Disconnect Peer Answer) lo que supondrá la desconexión de la capa de transporte. El agente que ha recibido la petición de desconexión, no deberá reconectarse de nuevo salvo una razón de peso. Las posibles causas por las que un agente Diameter puede solicitar el fin de la conexión son:

- Rebooting (0): se va a producir un reinicio del agente.
- Busy (1): el agente no es capaz de gestionar sus recursos internos.
- DO_NOT_WANT_TO_TALK_TO_YOU (2): el agente ha determinado que no existe la necesidad de mantener establecida la conexión ni tampoco en un futuro.

2.3 Circuit Switched Fallback (CSFB)

Como llevamos mencionando desde el comienzo de este proyecto fin de carrera, las redes LTE proveerán todos los servicios utilizando el protocolo IP sin la necesidad de utilizar las funciones del dominio de circuitos. Las llamadas de voz y mensajes de texto, tradicionalmente provisionadas en circuitos, serán reemplazadas por el protocolo VoIP (Voice over IP). Será necesario entonces el despliegue de IMS (IP Multimedia Subsystem) como plataforma de control del servicio. Esto supondrá un gran cambio en

las arquitecturas de red de las operadoras de telefonía, y llevará tiempo adaptarlas al nuevo estándar.

Hasta entonces, aunque el usuario se encuentre registrado en la red LTE, deberá ser capaz de realizar o recibir llamadas y de recibir o enviar mensajes de texto. Aún hoy, los terminales móviles LTE que se encuentran bajo cobertura LTE, no pueden utilizar el acceso radio UTRAN de forma simultánea, esto significa, que el terminal móvil no podrá recibir o realizar llamadas de voz o disfrutar de los servicios de mensajería de texto.

Sin embargo, las llamadas de voz es uno de los servicios más importantes en las comunicaciones móviles y es realmente necesario poder seguir ofreciendo servicios de voz a los usuarios cuando se encuentran disfrutando de los servicios de datos de alta velocidad ofrecidos por LTE y no se han provisionado los servicios de voz en el subsistema IMS.

Ante tal reto, el organismo 3GPP decidió estandarizar un mecanismo por el cual las operadoras móviles serían capaces de ofrecer servicios de voz a pesar de no haber desplegado aún IMS en sus redes. Dicha funcionalidad se denomina Circuit Switched Fallback (CSFB).

El concepto básico de CSFB es la notificación de que el terminal móvil va a recibir una llamada de voz por el dominio de circuitos existente cuando se encuentra registrado en LTE. Cuando esto ocurre, el terminal móvil es redirigido al dominio 2G/3G para recibir la llamada de voz, y la llamada permanece en el dominio de circuitos hasta que es completada. La solución de CSFB es también utilizada cuando existe poca cobertura LTE en la zona en la que se encuentra el usuario.

En la siguiente figura podemos observar la arquitectura de CSFB.

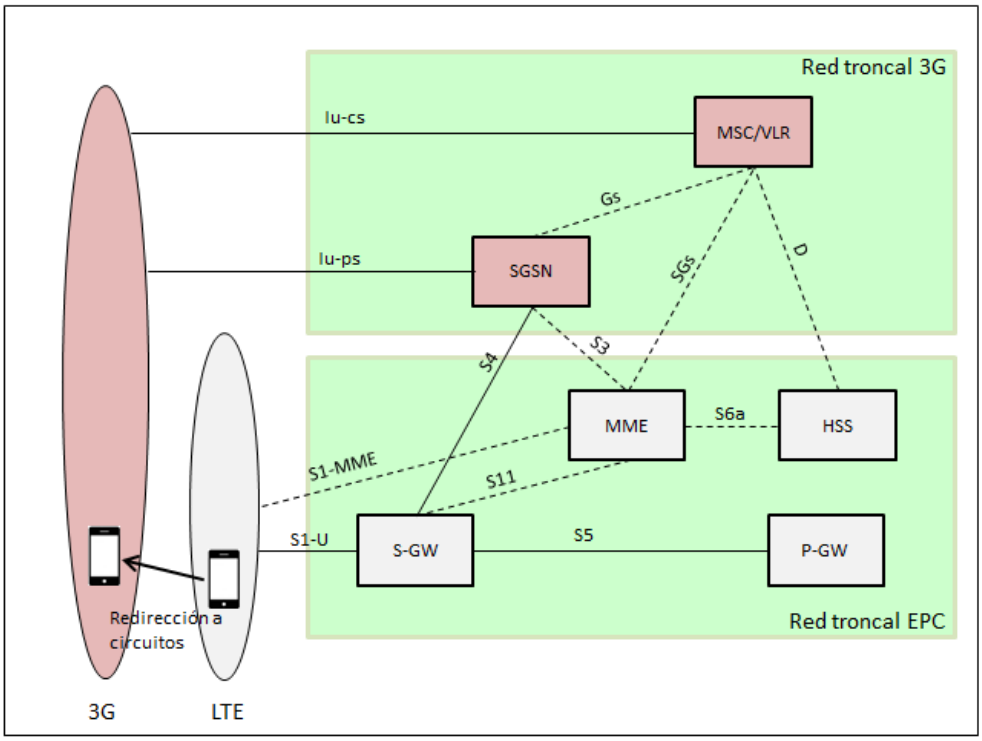

Figura 8: Arquitectura de red en CSFB

Una de las características más reseñables de las redes troncales que soportan CSFB es que la MSC (Mobile Switching Center) y VLR (Visited Location Register) del dominio de circuitos están conectados con el MME.

El interfaz que conecta la MSC y VLR con el MME se denomina SGs y es utilizado por la funcionalidad CSFB [6] para transferir las peticiones de llamadas terminantes desde el dominio de circuitos a la red LTE y para también la gestión de la movilidad del usuario cuando debe redirigirse al dominio 2G/3G.

Una red de comunicaciones móviles debe conocer en todo momento donde se encuentra localizado un terminal móvil para poder ofrecer los servicios móviles al usuario final. El procedimiento para determinar donde se encuentra un terminal es conocido como gestión de la movilidad (Mobility Management). Para completar una llamada usando la funcionalidad de CSFB, el dominio de circuitos necesita saber en qué área de localización se encuentra el terminal móvil.

Cuando un terminal móvil está utilizando LTE no puede usar 3G, esto implica que el MME, el cual contiene el área de seguimiento (TA, Tracking Area) en la que se encuentra el usuario, será incapaz de identificar a que MSC/VLR debe enviar los mensajes de gestión de la movilidad. Para solucionar este problema, el MME deberá mapear las áreas de seguimiento del usuario en LTE con las áreas de localización (LA, Location Area) de 2G/3G, es decir, a partir del area de seguimiento en la que se encuentra el usuario, sabrá qué área de localización y MSC/VLR le corresponde tal y como se muestra en la siguiente figura.

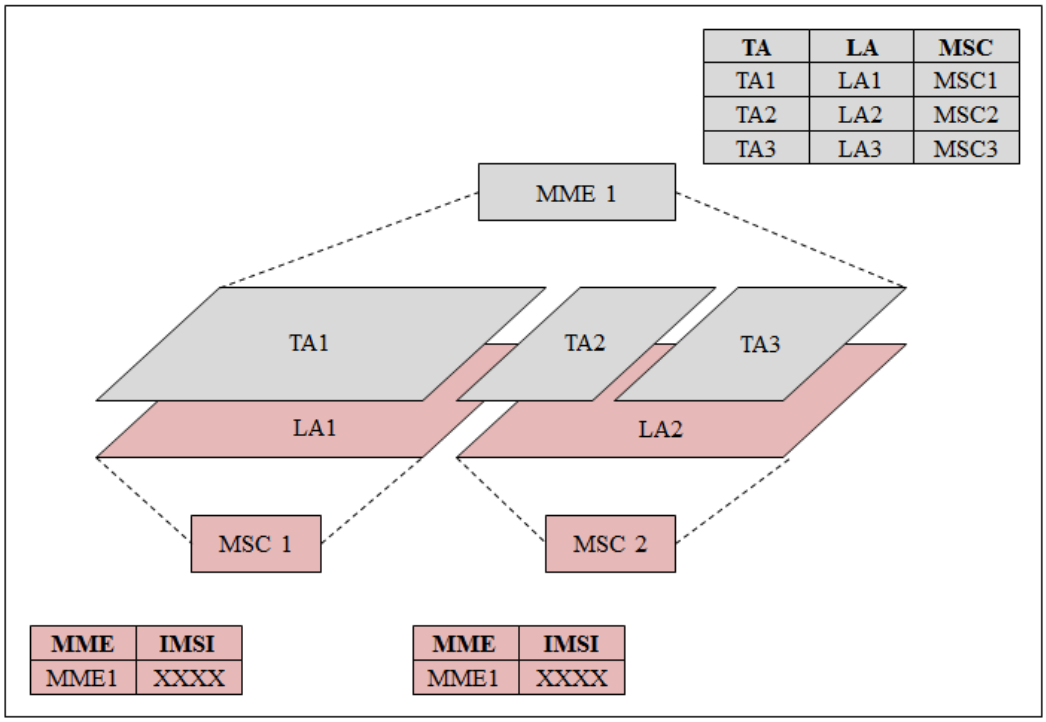

Figura 9: Mapeo área de localización con área de seguimiento

El procedimiento de movilidad combinado para la actualización del área de seguimiento y área de localización en CSFB es realizado por el MME de la siguiente manera:

- El terminal móvil envía al MME una petición de actualización del área de seguimiento (TAU, Tracking Area Update) indicando el área de localización en la que se encuentra actualmente.

- El MME lanza un procedimiento actualización de la localización hacia el HSS para obtener el área de localización del usuario.

- El MME, a partir del área de seguimiento es capaz de identificar la correspondiente área de localización y la MSC/VLR que controlan esa área y utiliza el interfaz SGs para enviar una petición de actualización del área de localización (LAU, Location Area Update) a la MSC/VLR con el área de localización asociada.

- La MSC/VLR guarda la correspondencia entre el identificador del MME y el IMSI que identifica al subscriptor, de esta manera, la MSC/VLR sabrá en que MME está el usuario actualmente conectado y que se encuentra en LTE.

- La MSC/VLR realiza un procedimiento de registro de localización hacia el HSS e informa al MME de la identidad temporal del usuario (Temporary Mobile Subscriber Identity, TMSI) que es utilizada para llamadas en el dominio de circuitos y para indicar que la localización del registro ha sido completado.

- Por último, el MME informará al terminal móvil que ha sido registrado mediante un procedimiento combinado de localización.

De forma muy breve, describiremos como es el procedimiento del CSFB en llamadas, tanto originantes como terminantes.

2.3.1 Llamadas de voz originantes

Para originar una llamada de voz utilizando la funcionalidad de CSFB, el terminal móvil que se encuentra registrado en un área de localización LTE, debe primero re dirigirse a la red 2G/3G. Para ello, debe enviar una petición de redirección a circuitos al MME. No debemos olvidar que la portadora o camino para la transmisión de datos siempre presente en la red troncal, debe también transferirse. El MME, para cumplir con dicho requisito, envía una petición de transferencia al terminal móvil para que cambie la red de acceso radio de LTE a 2G/3G. Una vez se ha realizado la transferencia, el terminal móvil envía una petición de servicio de voz al MSC/VLR para que se establezca la conexión que se utilizará para realizar la llamada.

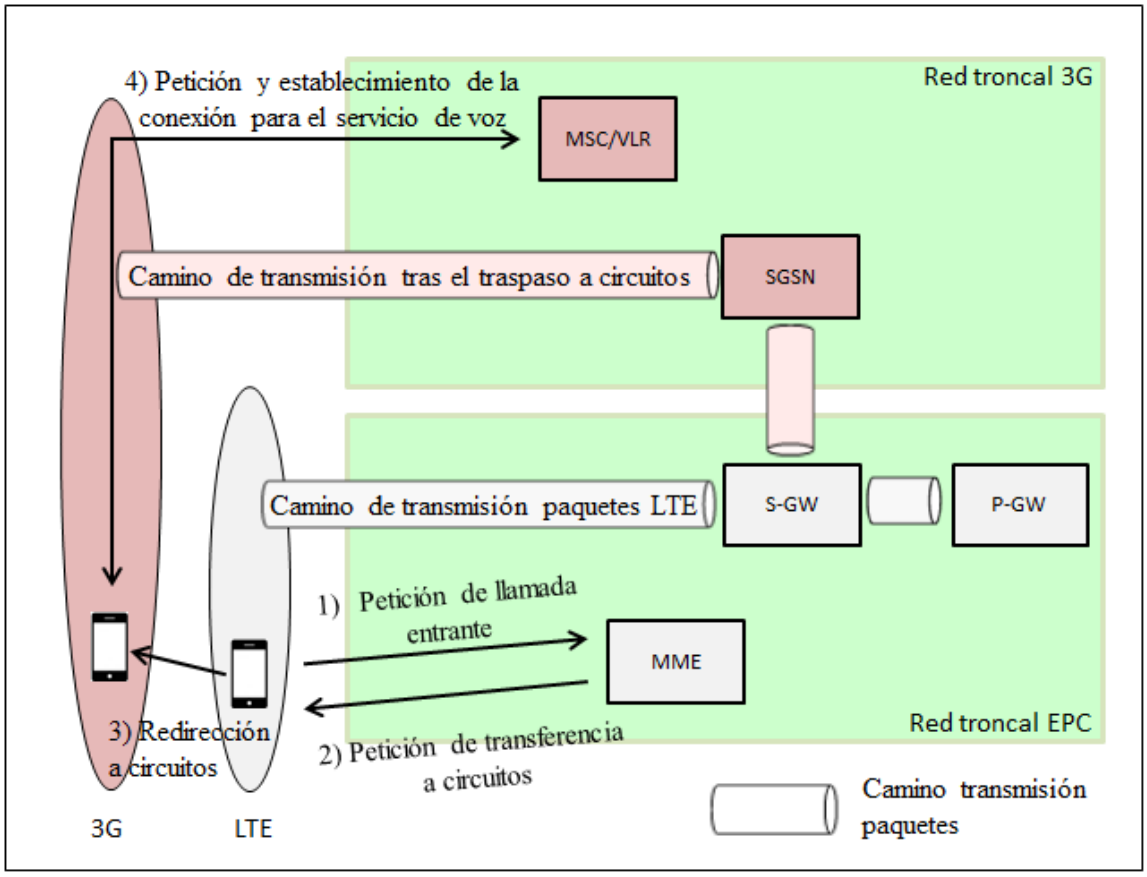

Figura 10: Llamada originante en escenario de CSFB

2.3.2 Llamadas de voz terminantes

Cuando la MSC/VLR recibe un mensaje indicando la llamada de voz, es capaz de identificar el MME asociado al usuario a partir de la información recibida en la llamada,

es decir, a través del IMSI. A continuación, el MME envía un mensaje de notificación al terminal móvil en LTE indicando que la llamada es un servicio de conmutación de circuitos, así que el terminal móvil envía una petición de CSFB al MME. Una vez realizado el traspaso, el terminal se encuentra en 2G/3G y envía un mensaje de notificación a la MSC/VLR en la cual está registrado y la llamada de voz es ejecutada.

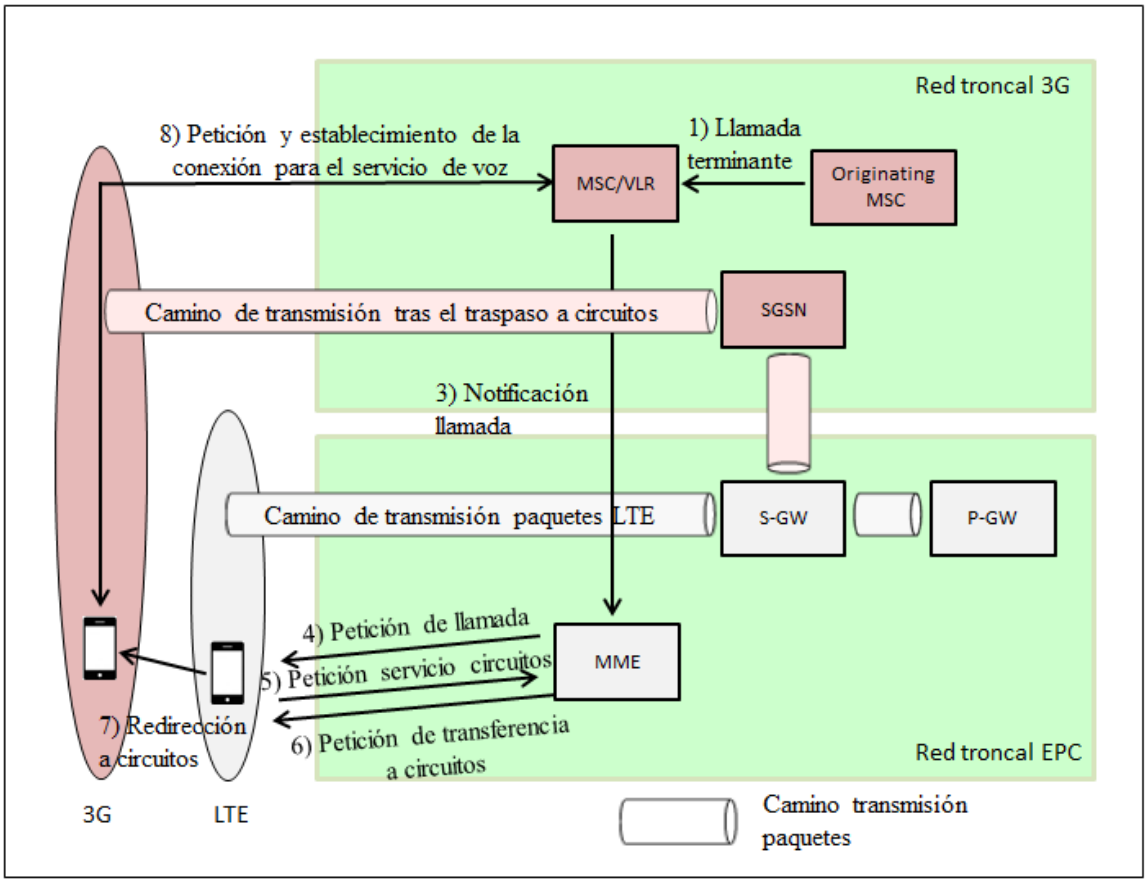

Figura 11: Llamada terminante en escenario de CSFB

2.3.3 Des alineamiento de área de seguimiento y área de localización

Aunque ya hemos hecho mención a la correspondencia entre área de seguimiento y el área de localización realizada durante el proceso de gestión de la movilidad, la funcionalidad de CSFB confía en el exhaustivo emparejamiento que se lleva a cabo.

Errores en este mapeo debidos a factores radio pueden provocar que un terminal móvil se registre en una MSC/VLR que no le corresponde.

Normalmente, las comunicaciones no pueden realizarse si una llamada originante o terminante es atendida por una MSC/VLR en la que el terminal móvil no se ha registrado de forma correcta.

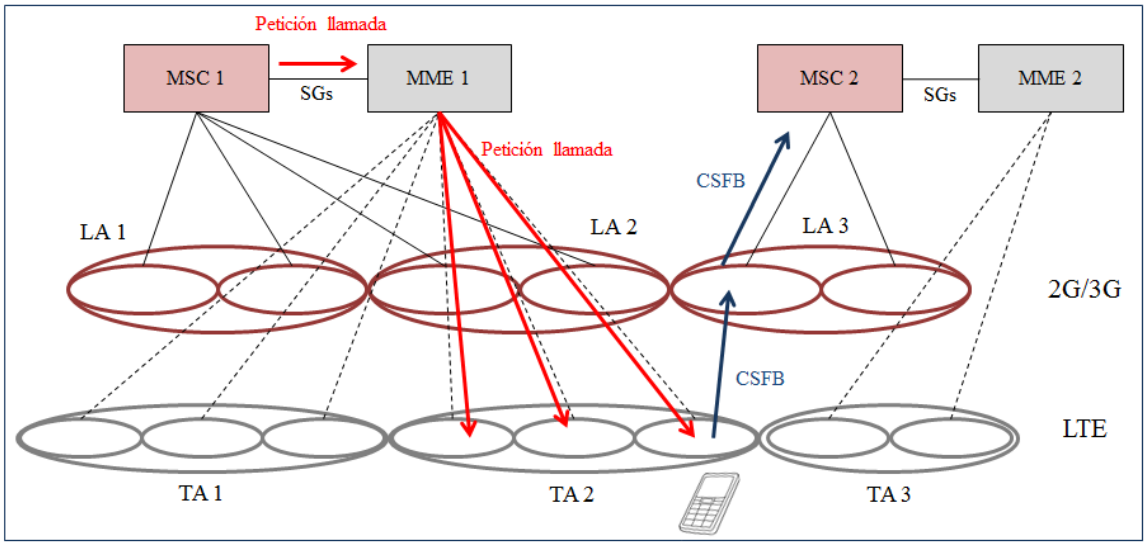

Figura 12: Des alineamiento área de seguimiento y área de localización

En la figura anterior vemos que el terminal móvil está registrado bajo el área de seguimiento 2 del MME 1 y del área de localización 2 de la MSC 1 cuando recibe la petición de una llamada terminante.

Dependiendo de la localización geográfica del terminal, cuando hace el traspaso a la red 2G/3G, puede seleccionar registrarse en el área de localización 3 que depende de la MSC 2. En esta situación, el terminal enviará una respuesta a la petición de CSFB a la MSC 2 que no está informada del establecimiento de la llamada y no tiene el perfil de subscripción del usuario, así que la llamada terminante fallará.

Para solucionar este problema, el procedimiento *"Roaming Retry"* ha sido adoptado en CSFB. Después de recibir la petición CSFB y re dirigirse a la red 2G/3G, el terminal móvil envía la respuesta a la petición de CSFB a la MSC2 con un registro de localización que no ha ocurrido. Como el MSC2 no puede determinar a qué se debe esa respuesta, devuelve un mensaje de rechazo al terminal móvil. Este mensaje de rechazo inicia un nuevo procedimiento de actualización del área de localización que es enviado a la MSC que da servicio al área de localización en la que se encuentra el terminal, en este caso, la MSC 2. Esta nueva MSC realiza los procedimientos de actualización de la localización contra el HSS que harán que se borre de la base de datos la información que existía sobre la información de localización.

No es realístico pensar que las coberturas LTE y 2G/3G coincidirán de manera perfecta, esto solo ocurriría si existiese un único conjunto de MSCs y MMEs que diesen servicio a toda la red.

Capítulo 3

Itinerancia Internacional

Continuamos con el desarrollo de conceptos claves necesarios para la realización de este proyecto final de carrera. Entenderemos que es la itinerancia internacional, conceptos asociados a ella, que tipos de arquitecturas de red se pueden implementar, cómo se interconectan las redes de dos operadoras para ofrecer servicio de itinerancia internacional a usuarios que se encuentran en su red. En la sección final, profundizaremos en cómo se produce el registro de un usuario en red, que entidades participan y cuáles son los mensajes que se intercambian.

3.1 Qué es la itinerancia y definiciones básicas

La itinerancia o roaming es la capacidad que posee un usuario móvil para acceder a los servicios de llamadas, datos o mensajes de texto a través de la red de otro operador sin necesidad de utilizar otra tarjeta USIM [7]. Es especialmente útil cuando el usuario se encuentra en el extranjero, aunque también se puede utilizar a nivel nacional cuando un operador no dispone de cobertura en determinadas zonas del país.

Si la red visitada está en el mismo país del que procede el usuario, se conoce como itinerancia nacional, pero si la red visitada está fuera del país de la red propia, se conoce como itinerancia internacional.

En este proyecto fin de carrera trataremos exclusivamente el servicio de itinerancia internacional y a continuación exponemos distintas técnicas utilizadas para proveer el servicio de itinerancia internacional a los usuarios:

- **Itinerancia estándar bilateral**: es la relación bilateral común entre dos operadoras que han firmado el acuerdo de roaming internacional (IRA, International roaming agreement) y han seguido los procedimientos de pruebas básicos a la apertura de acuerdo. El operador utiliza tarjetas USIM ("Universal Subscriber Identity Module") con IMSIs ("International Mobile Subscriber Identity) pertenecientes su rango de numeración para registrarse en la red del operador con la que tiene el acuerdo comercial de itinerancia.

  Esta técnica es utilizada prácticamente por la totalidad de las operadoras móviles.

- **Soluciones de IMSI dual (Inter standard roaming)**: permiten a un operador A usar el rango de IMSI del operador B y conseguir acceso a las redes de los socios de itinerancia del operador B. El operador A utilizará SIMs con IMSI dual, es decir, en territorio nacional utiliza su propio IMSI, pero cuando se encuentra en el extranjero, utilizará el rango de IMSI del operador B.

  Al no ser necesaria la realización de las pruebas previas a la apertura del acuerdo de itinerancia, esta solución provee rápidamente de acuerdos de itinerancia al operador A.

- **Centro gestores de itinerancia**: el operador se conectará a un concentrador de itinerancia internacional en el que delega la mayoría de las funciones asociadas a las aperturas de acuerdos comerciales, para hacerlas más eficaces y ágiles.

  Los concentradores de itinerancia serán tratados en el capítulo 4 de este proyecto fin de carrera.

La itinerancia internacional está soportada técnicamente por los procedimientos de movilidad, autentificación y tarificación.

El establecimiento de la itinerancia entre operadores está basado en acuerdos de itinerancia donde se incluyen los términos comerciales asociados. El acuerdo estándar de la asociación GSMA está compuesto por los denominados AA.12, AA.13 y AA.14. Aunque el término general es acuerdo de itinerancia bilateral, puede ser en realidad bilateral o unilateral, es decir, que sólo uno de los socios de itinerancia podrá hacer uso de los servicios en la red del otro.

El AA.12 fija el marco legal básico para las relaciones de itinerancia internacional bilaterales. Cubre áreas tales como la confidencialidad, privacidad de los datos, responsabilidades, prevención del fraude, duración del acuerdo, suspensión y finalización de los mismos.

Los AA.13 y AA.14 son suplementarios al marco legal básico. Contienen principios prácticos y procedimientos que las operadoras deciden implantar en el acuerdo.

El AA.13 es el documento permanente de referencia o PRD (Permanent Reference Document) que forma parte de la base de las operaciones y procedimientos diarios de la itinerancia. En él se acuerdan los servicios que serán implementados, siempre de acuerdo a las especificaciones relevantes, los detalles de la tarificación y procedimiento de pago, la gestión de los clientes y aspectos técnicos que incluyen desde el uso de las tarjetas de pruebas, temas de seguridad y conexiones entre redes. En el caso de que se decida implementar un acuerdo sobre el nivel de servicio de itinerancia, debe ser incluido en el anexo C.12 con el objetivo de garantizar la calidad de servicio entre ambas redes.

El AA.14 contiene la información específica al operador clasificada en dos áreas principales:

- "Confidencial del operador": contiene información sensible como las tarifas entre operadores (IOTs, Inter-Operator-Tariffs) y contactos para ciertos procesos de negocio, como la transferencia de ficheros de tarificación, intercambio de facturas y teléfonos de atención al cliente para contactos entre operadoras.

- "Dominio público": incluye la lista de servicios ofrecidos, números de atención al cliente para el uso de los clientes e información general de atención al cliente.

Fases de la apertura comercial

El proceso de apertura comercial de un acuerdo de itinerancia se divide en dos fases fundamentales:

- En la fase pre-comercial se negocia el acuerdo comercial y la red y las entidades de red son configuradas y probadas adecuadamente.

- Cuando estas actividades se completan satisfactoriamente, el servicio de itinerancia comercial puede empezar y los clientes pueden usar las redes y servicios del otro operador.

A lo largo del capítulo serán descritas las dos implementaciones que se pueden realizar en el escenario de itinerancia internacional. Todo dependerá de la interconexión realizada entre las redes de las operadoras, es decir, la red de la que procede el usuario, a la que llamaremos red local y la red del país extranjero en el que se encuentra, a la que denominaremos red visitada.

Es necesario que conozcamos un par de definiciones más muy utilizadas en el mundo de la itinerancia internacional:

- "Inbound roaming" o tráfico de itinerancia entrante. Se utiliza este término para designar a aquel tráfico de itinerancia internacional generado por usuarios que pertenecen a otras operadoras pero se encuentran registrados en nuestra red.

- "Outbound roaming" o tráfico de itinerancia saliente. Lo utilizamos para referirnos al tráfico generados por nuestros abonados en redes móviles extranjeras.

3.2 Arquitectura de la una red LTE en itinerancia

Una vez conocidos los elementos que conforman una red LTE, tal y como hemos visto a lo largo del capítulo 2, describiremos ahora los dos modelos de implementación que existen para el servicio de itinerancia internacional, ambos definidos por el estándar 3GPP [8] y ya existentes en las redes 2G/3G.

Debemos distinguir entre dos escenarios:

- **Home Routed**, el tráfico de voz y datos es gestionado por la operadora de la que el usuario es originario.

- **Local Break Out (LBO)**, el tráfico de voz y datos es gestionado por la operadora de la red visitada.

Antes de pasar a describir de forma más extensa cada uno de los modelos, en la siguientes figuras veremos de forma sencilla la diferencia básica entre ellos, es decir, qué operadora, local o visitada lleva el control del tráfico de voz en primera figura y de datos en la segunda.

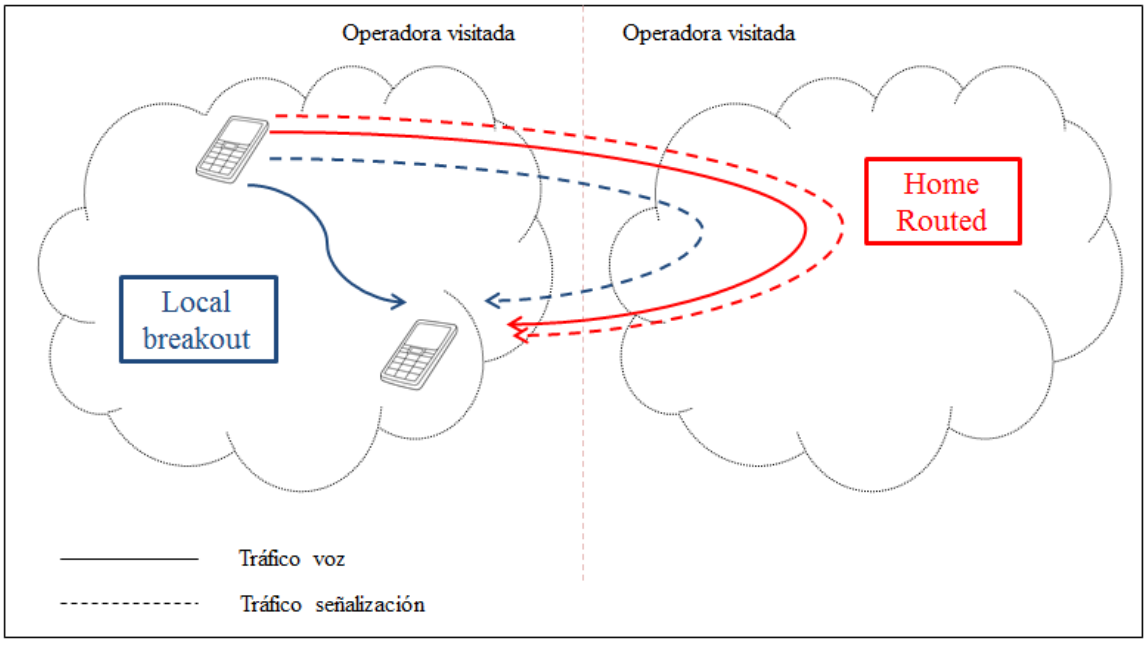

Figura 13: Escenario de itinerancia internacional para tráfico de voz

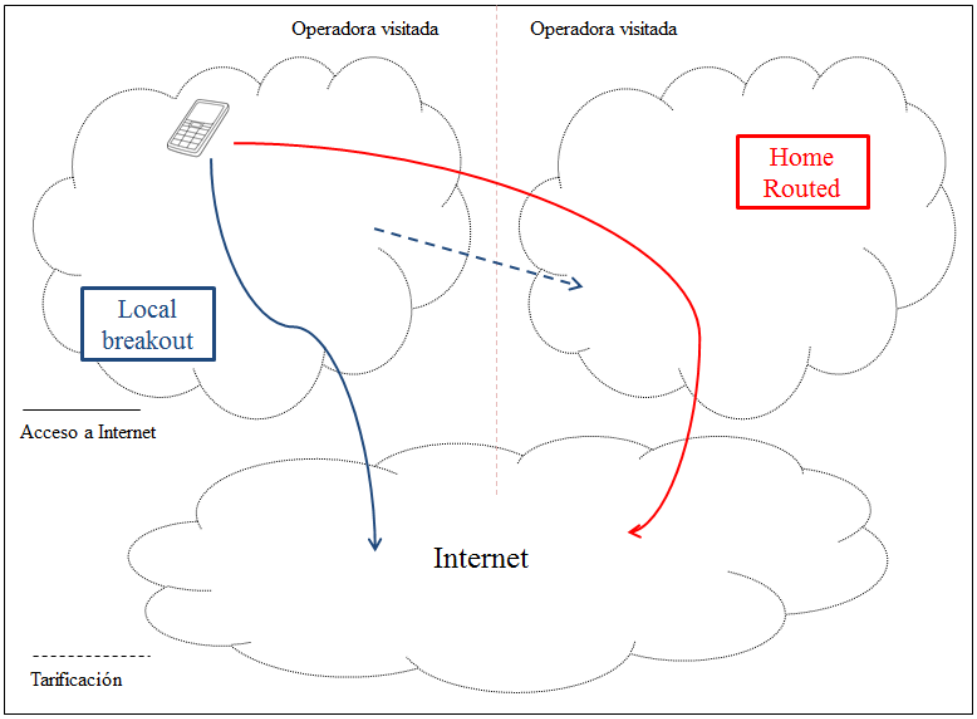

Figura 14: Escenario de itinerancia internacional para tráfico de datos

Aunque los dos modelos se pueden implementar técnicamente, el modelo Home Routed es el más extendido entre las operadoras.

El escenario de Local Break Out supone uno de los retos de la nueva regulación europea y será desarrollado en el capítulo 7.

3.2.1 Home Routed

Este modelo de arquitectura, no difiere mucho de la arquitectura EPC descrita en la figura 15 del capítulo 2. Las diferencias básicas son que el S-GW está localizado en la red visitada, mientras que el P-GW está localizado en la red de origen y que el interfaz entre ambos nodos de red se ha sustituido por el interfaz s8.

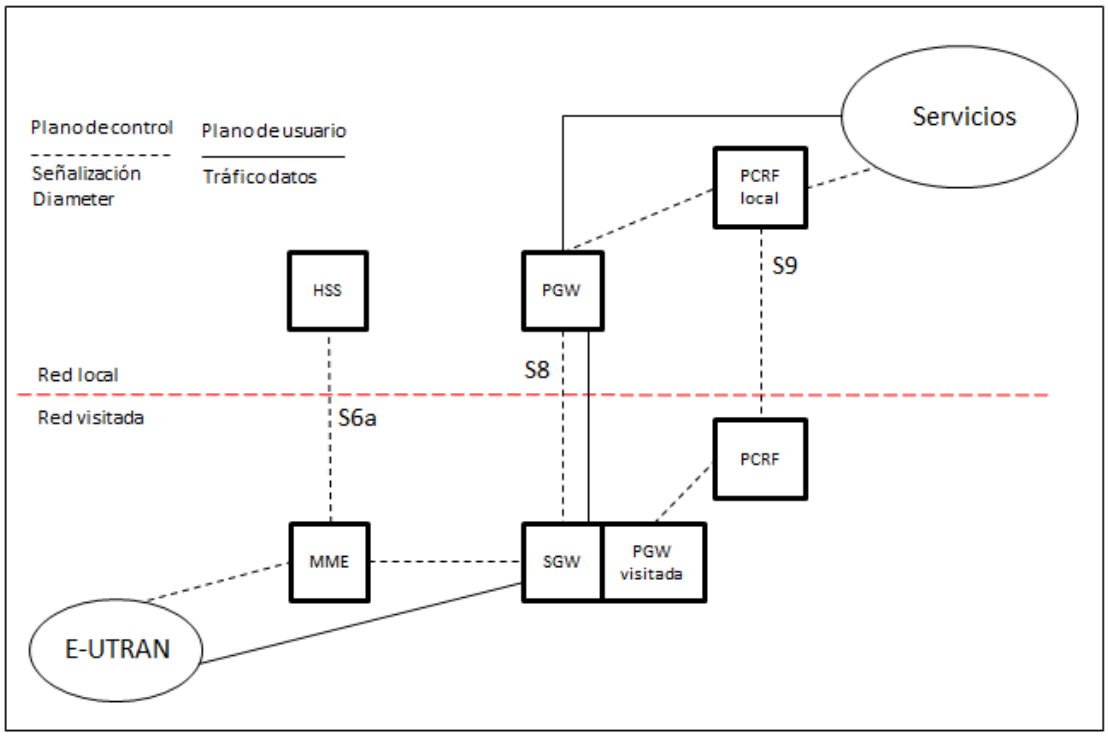

Figura 15: Implementación Home Routed

Una vez el usuario se ha autenticado en la red visitada, todo su tráfico será enrutado desde el SGW hasta el PDN de su red local para alcanzar Internet, es decir, sus sesiones de datos serán reencaminadas desde la red visitada a la red origen.

Este modelo de arquitectura es recomendado cuando la relación entre ambos operadores no es de plena confianza, pues el operador de origen tiene un gran control sobre el tráfico del usuario. Pero es un modelo que hace incrementar los costes para la operadora,

3.2.2 Local Break Out: Itinerancia con desvío local

El usuario se conecta a internet y a los servicios sin enrutar el tráfico a su red origen, sino que se conecta a éstos a través de la red Visitada. El PRCF de la red origen pide permiso para utilizar el PGW de la red visitada, así que la autenticación es realizada en el interfaz que une estos nodos de red, el interfaz s9.

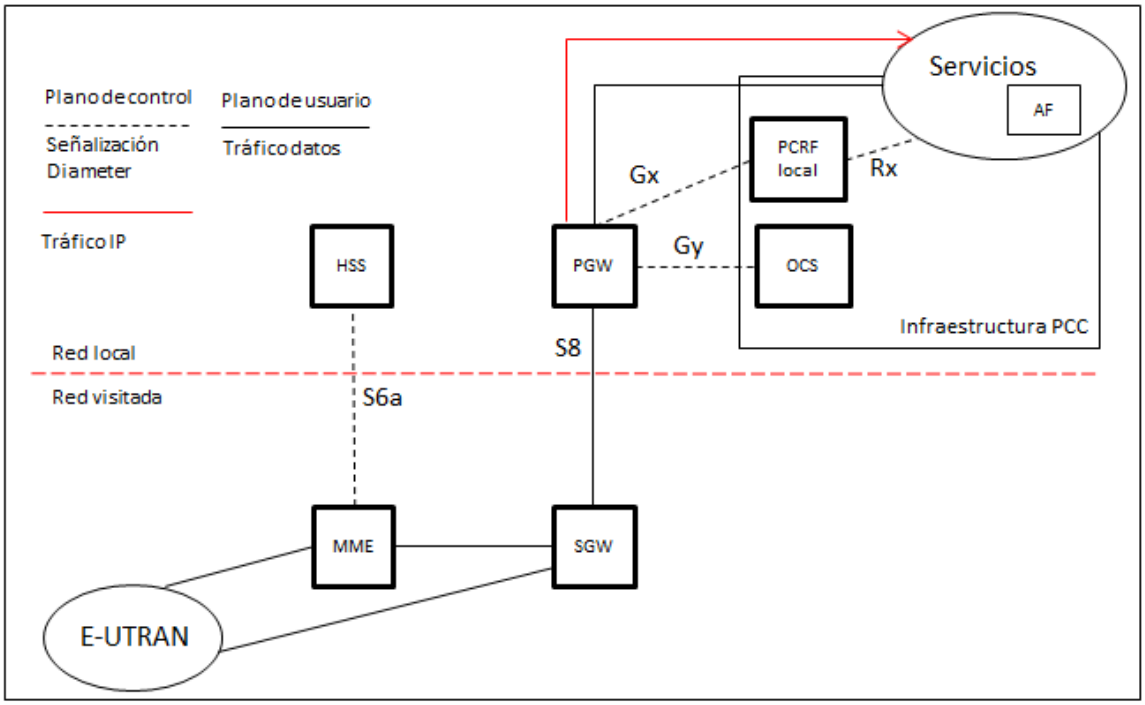

Figura 16: Implementación Local Break Out

El Local breakout es un tema emergente y que está atrayendo la atención de los mercados de las operadoras móviles, pero aún su futuro es incierto, principalmente porque la operadora con este tipo de implementación pierde el control del tráfico de sus usuarios, aunque los costes se reducen y se mejora la calidad del servicio ofrecido. Aun así, produce gran desconfianza en las operadoras.

3.3 Interconexión de redes LTE en itinerancia: centralización

Como se ha descrito en la sección anterior, en la red troncal LTE existen diferentes interfaces de señalización basados en el protocolo Diameter que conectan elementos de red de la red visitada, MME, S-GW y vPCRF, con los elementos equivalentes en la red local, HSS, P-GW y vPCRF, para hacer posible el servicio de itinerancia internacional entre ambas operadoras. Con el rápido crecimiento de terminales LTE, y la evolución o sustitución de la señalización SS7 por Diameter, las redes se han visto obligadas a desplegar más de una instancia de los elementos mencionados, para poder dar servicio a todos los usuarios, lo que ha provocado un aumento importante de señalización y conexiones punto a punto a implementar entre ambas redes y dentro de la propia red, por lo que la interconexión de ambas operadoras puede no ser un trabajo fácil por las tareas de administración y configuración y control constantes que deben realizarse.

Este tipo de arquitectura mallada se está convirtiendo en un problema cuando el operador desea expandir y mantener su red tanto a nivel interno como cuando quiere interconectarse con otra operadora.

En la siguiente figura podemos observar la cantidad de conexiones punto a punto que deben implementarse, y el número puede ir aumentando progresivamente en función del despliegue de nuevas entidades en cualquiera de las redes.

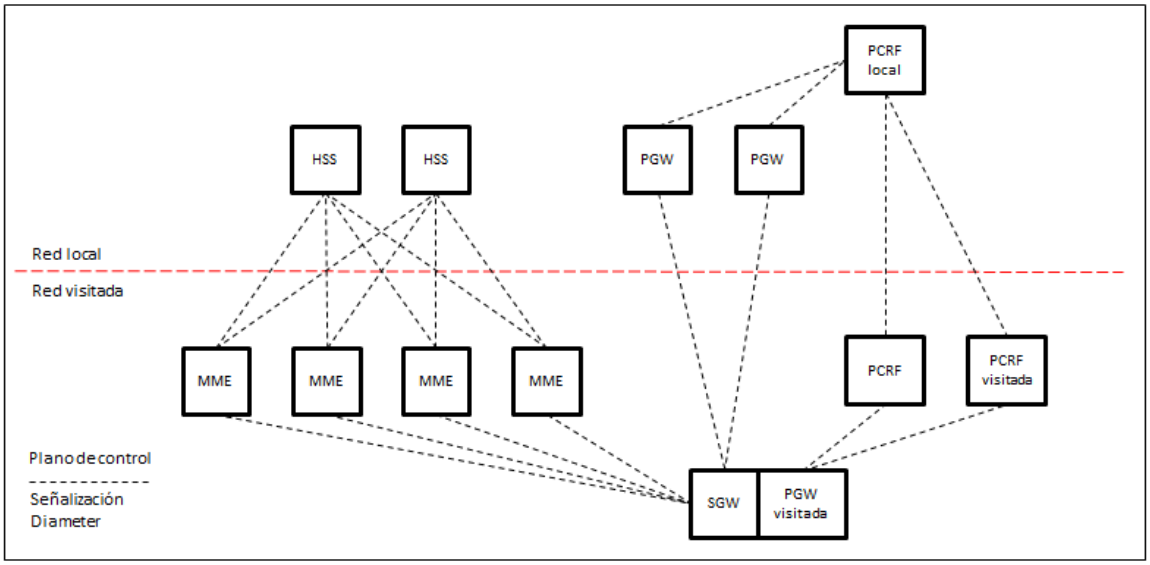

Figura 17: Interconexión redes en itinerancia internacional

Para simplificar el interfaz de roaming entre ambas operadoras, una nueva entidad funcional, un agente Diameter, denominado DEA (Diameter Edge Agent) ha sido definido en las directrices de la GSMA sobre roaming LTE (GSMA PRD IR.88).

Los DEAs supondrán el único punto de acceso a la red en las interconexiones con las redes de sus socios de itinerancia internacional enmascarando la topología de red que hay por detrás para no exponer sus elementos a las redes externas. Informarán también que ellos son el agente Diameter que se encuentra manejando el tráfico de señalización para la operadora, pudiendo ser un agente de tipo relay o de tipo proxy. Además se encargarán de otras funcionalidades como el control de admisión y acceso a la red, políticas de control y manipulación de los mensajes recibidos para añadir información valiosa cuando se realice el enrutado del mensaje.

Existen dos implementaciones básicas para la interconexión de dos operadoras en función de la conectividad IP existente entre ellas:

- Interconexión directa entre los agentes Diameter (DEAs) de las dos operadoras, representada en la figura 18.

- Interconexión de las operadoras a través de los agentes Diameter de un IPX (IP Packet Exchange). Los IPX proveen del servicio de conectividad IP entre los operadores móviles que no poseen de un DEA en su red como se puede observar en la figura 19.

Desde la perspectiva de la red, el DEA mejorará el rendimiento y la escalabilidad de la red, proporcionando estabilidad cuando se producen avalanchas de tráfico de señalización. Concentrarán las conexiones punto a punto que deben establecerse entre

todas las instancias que conforman el núcleo de la red de la operadora, pudiendo realizar labores de balanceo de carga para no sobrecargar ningún nodo de red en concreto. Otras de las funciones básicas de estos nodos

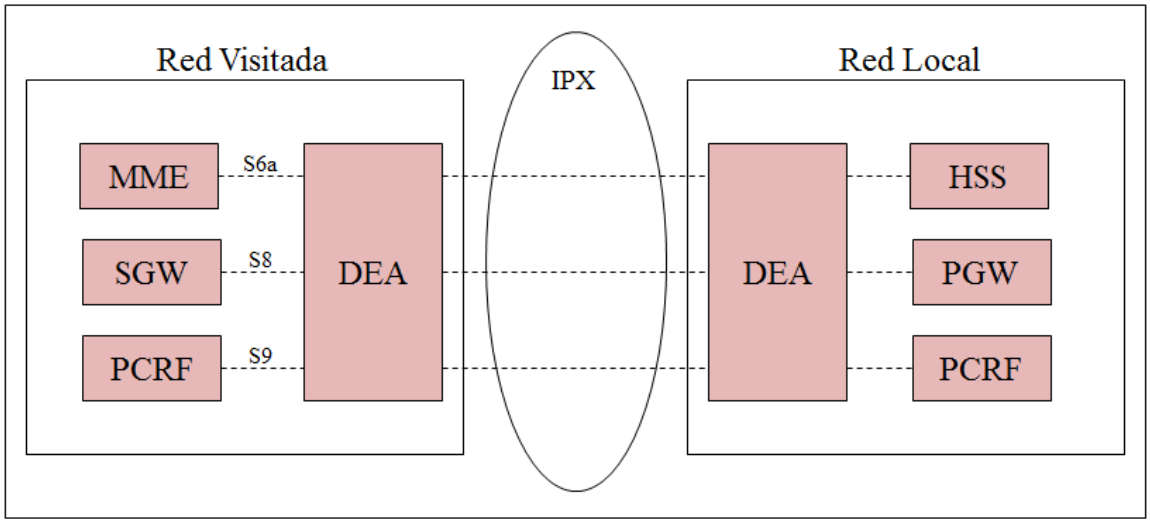

Figura 18: Interconexión directa redes LTE

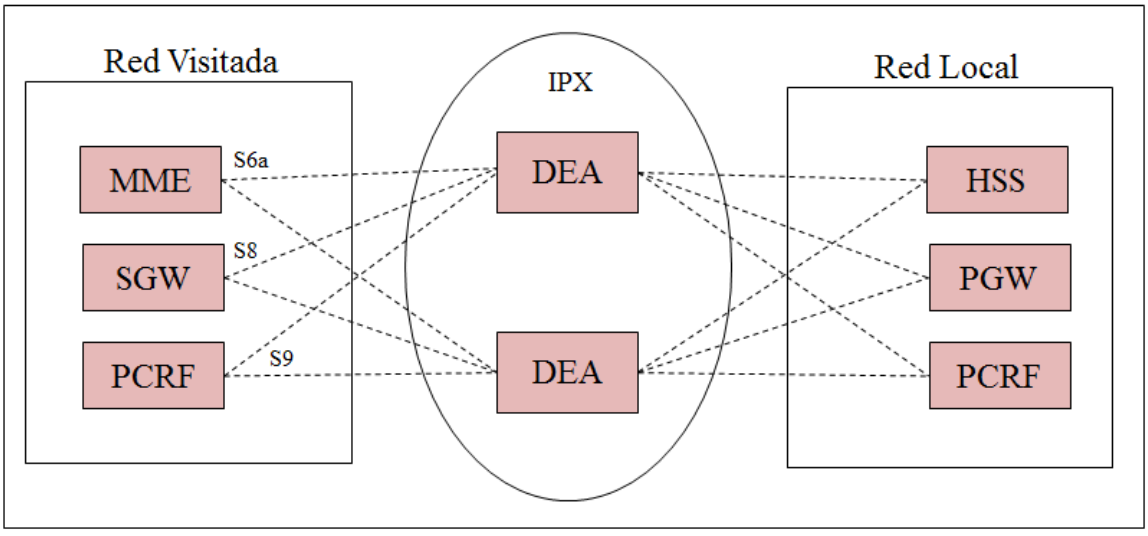

Figura 19: Interconexión redes LTE a través de un IPX

3.4 Registro de usuarios en LTE roaming

Los clientes de las operadoras móviles cuando encienden su terminal móvil o se encuentran en una red visitada, realizan un procedimiento de registro en la red para comenzar a disfrutar de los servicios como llamadas, mensajería o datos independientemente de la red en la que se encuentren.

La figura 20 obtenida de la especificación TS 23401 muestra el flujo de mensajes completo para registrar un usuario en la red.

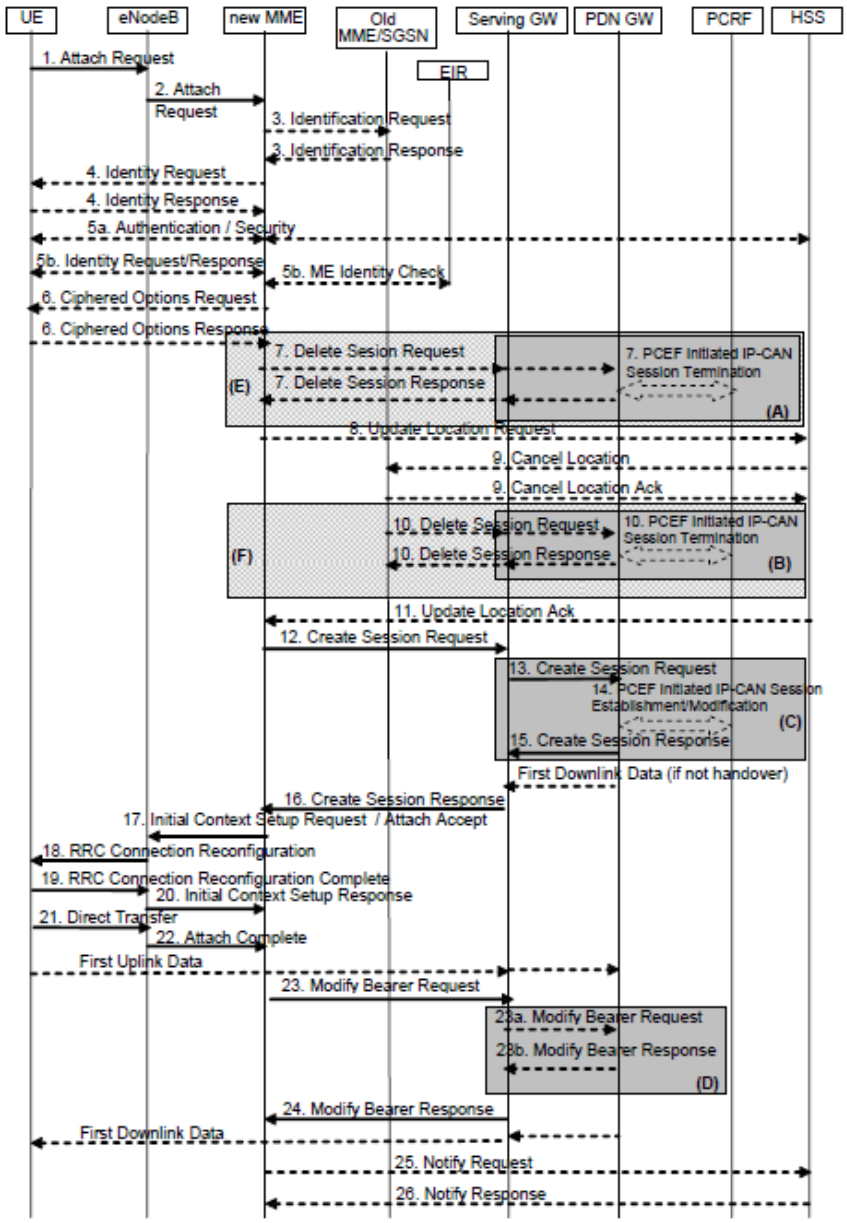

Figura 20: Registro de usuario en red LTE completo

Nosotros sin embargo, estudiaremos un escenario más simplificado, donde prestaremos toda nuestra atención a los mensajes intercambiados en el interfaz S6a, es decir, el segmento localizado entre el MME y el HSS. Para ello, nos basaremos en un escenario más sencillo mostrado en la figura 21.

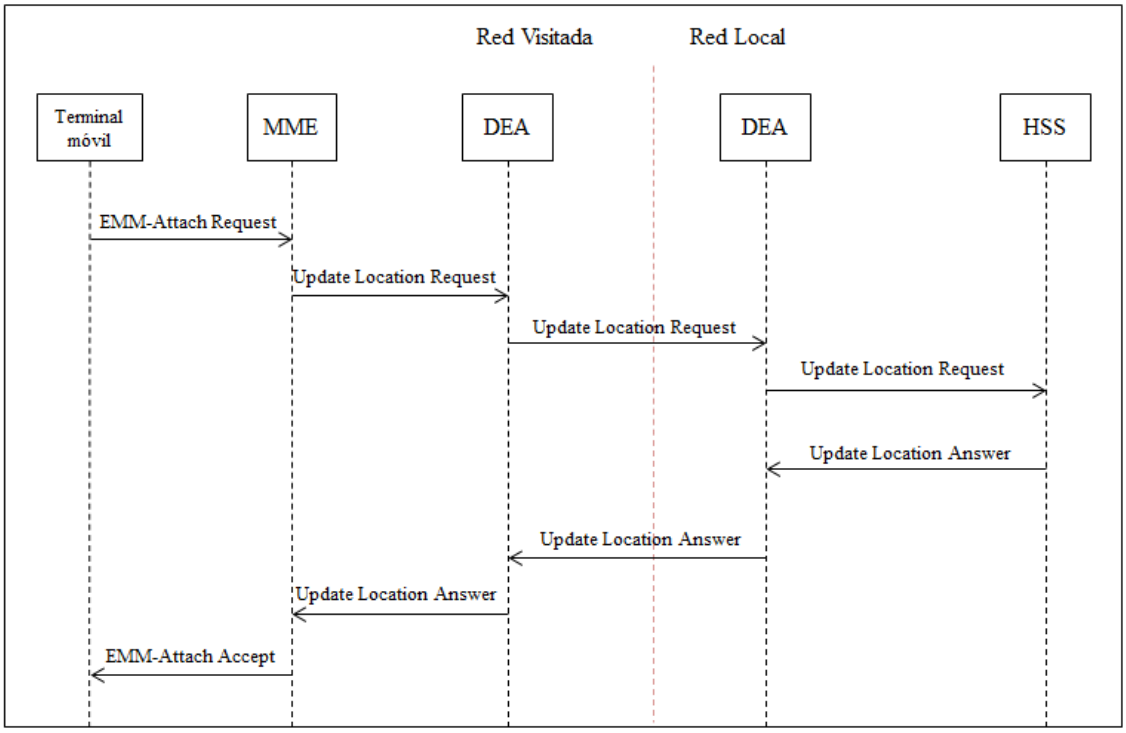

Figura 21: Registro de usuario en red LTE simplificado

El terminal móvil iniciará el registro en la red lanzando un mensaje de "Attach Request" con el IMSI del usuario contra el MME. Éste, una vez almacenado el IMSI, debe continuar con el registro del usuario en la red y debe descubrir los servicios que puede utilizar.

El procedimiento de "Update Location" debe realizarse entre el MME y el HSS a través del interfaz S6a, basado en el protocolo de señalización Diameter, para actualizar la información de localización del usuario en el HSS [9]. Dicho procedimiento es siempre iniciado por el MME y lo utiliza para:

- Informar al HSS que el usuario se encuentra bajo su área de cobertura.
- Descargar toda la información disponible en el HSS sobre la subscripción del usuario a la red.
- Actualizar el HSS con nueva información sobre el usuario como información relativa al terminal móvil.

Este procedimiento es mapeado en los comandos "Update Location Request (ULR)" y "Update Location Answer (ULA)" del protocolo Diameter.

Una vez el HSS recibe en "Update Location Request" por parte del MME, comprobará si existe información de subscripción para el IMSI indicado. Dependiendo del resultado de la comprobación, el HSS contestará al MME con un Update Location Answer y un código de resultado:

- Si el IMSI es conocido, el HSS enviará un ULA con código de resultado satisfactorio, DIAMETER_SUCCESS (2001).

- Si el IMSI no es conocido, el HSS enviará un ULA con código de resultado indicando que ha habido un error, DIAMETER_ERROR_UNKNOWN_USER_UNKNOWN (5001).

- Si el IMSI es conocido pero no le está permitido hacer roaming (por culpa de una restricción configurada en la red), el HSS enviará un ULA con código de resultado indicando que ha habido un error, DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004).

- Si el usuario está utilizando un tipo de acceso radio no permitido, el HSS enviará un ULA con el código de resultado DIAMETER_ERROR_RAT_NOT_ALLOWED (5421).

Cuando el MME recibe la contestación al Location Update Request por parte del HSS, debe chequear el resultado. Si es exitoso, almacenará el perfil de subscripción recibido así como la identidad del HSS que ha gestionado el registro.

Por último, se informará al usuario de que está registrado correctamente en la red.

3.4.1 Enrutamiento Diameter

Ya conocido el escenario del registro de un usuario en la red, vamos a seguir profundizando en cómo se lleva a cabo dicho procedimiento a nivel de señalización Diameter.

El enrutamiento de los mensajes Diameter hacia el destino final puede hacerse en función del realm de destino (destination-realm AVP), host de destino (destination-host AVP) o ambos a la vez. Como el host de destino no siempre es conocido, nos basaremos en el realm de destino para enrutar los mensajes. Necesitaremos también conocer las aplicaciones que soporta el terminal móvil.

La aplicación o aplicaciones se encuentran almacenadas en el AVP Application-ID y son obtenidas cuando se establece la conexión entre dos agentes Diameter mediante los comandos CER/CEA.

Usaremos el realm estándar definido en 3GPP 23.003 [10]:

“epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org”

Dónde el MNC (Mobile Network Code) es el código de identificación de la red móvil y el MCC (Mobile Country Code) es el código que identifica al país de la operadora móvil.
El agente Diameter es capaz de construir el realm a partir del MCC y MNC de la red móvil en la que se encuentra. En el caso de encontrarnos en escenarios de itinerancia internacional, para la construcción del realm de destino, el MME se encarga de almacenar el IMSI del terminal móvil en el AVP “User-Name”.

El IMSI está compuesto por 15 cifras, dónde las 3 primeras se corresponden con el MCC y las 2 o 3 siguientes son el MNC. Si se trata de una red dónde el MNC tan solo consta de 2 cifras, añadiremos un cero al comienzo del MNC a la hora de construir el realm.

El host que identifica al agente Diameter es muy fácil de construir pues tan sólo se trata de un identificador seguido del realm de la red en la que se encuentra el agente. La estructura sería la siguiente:

XXX.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Los agentes Diameter se ayudan de dos tablas para el enrutamiento de los mensajes hacia el destino:

1) Tabla de compañeros: se almacena información sobre los nodos Diameter a los que está el agente conectado, el estado en el que se encuentran, información de seguridad sobre ellos o si fueron configurado de forma estática o dinámica.
   Es la tabla utilizada para el reenvío de los mensajes y es referenciada por la tabla de enrutamiento.

2) Tabla de enrutamiento basado en el realm: se almacena el nombre del realm, el identificador de la aplicación, el tratamiento que se le debe hacer al mensaje y si la entrada en la tabla fue configurada de forma dinámica o estática.

Cuando el agente Diameter recibe un mensaje, chequea en su tabla de enrutamiento el realm de destino, la aplicación y que debe hacer con el mensaje. Las siguientes acciones pueden producirse:

- El realm de destino coincide con el realm del agente Diameter así que lo tratará localmente y no será enviado a ningún otro agente.

- El realm de destino no coincide con el suyo propio, así que será enviado al siguiente agente Diameter y dependiendo de si es un agente relay, proxy o redirect, podrá modificar la información de enrutamiento o la totalidad del mensaje.

Una vez el agente Diameter conoce qué debe hacer con el mensaje, chequeará en su tabla de compañeros cual es el agente al que debe reenviar el mensaje Diameter para que lo haga llegar a su destino.

Cuando hay que encaminar las respuestas al nodo que originó la petición, no hará falta chequear ninguna de las dos tablas anteriores, tan sólo con los AVP “End-to-End” y Hop-by-Hop” seremos capaces de enrutarlas al origen. Cuando la petición es reenviada por los diferentes agentes Diameter, el AVP “End-to-End” nunca cambia, pero se almacena, al igual que el AVP “Hop-by-Hop”, que también es almacenado pero en este caso si es reemplazado por un nuevo valor. Cuando los agentes Diameter reciban la respuesta, podrán reemplazar el AVP “Hop-by-Hop” por el que tienen almacenado y enviarán la respuesta al agente Diameter del cual recibieron la petición original.

En la siguiente figura podemos observar de nuevo proceso de registro del usuario en la red de forma más detallada. Se han obtenido las trazas de un entorno de maqueta gracias

a un simulador de tráfico. Los DEAs son nodos reales, mientras que el MME y el HSS son nodos simulados, así que en el caso de la red local, se ha utilizado un MCC y MNC que no pertenecen a ninguna operadora móvil real.

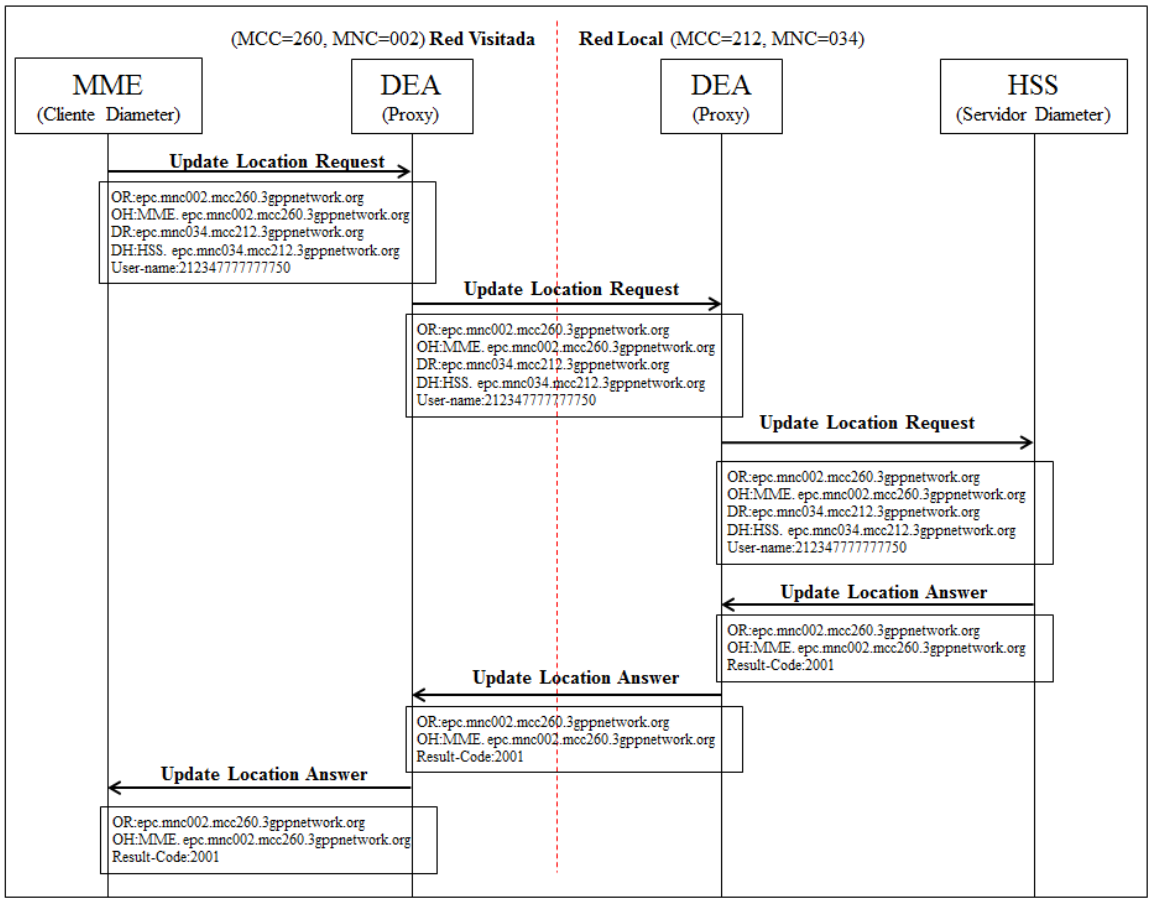

Figura 22: Registro de usuario en red detallado a nivel Diameter

El MME es el nodo Diameter que ejerce como cliente pues es el que genera la petición de mensaje, en este caso, un Update Location Request para registrar al usuario en la red. A partir del IMSI del usuario que tiene almacenado, puede generar el realm de destino al que quiere destinar el mensaje. El host de destino, si lo tiene almacenado también lo incluirá en el mensaje, sino, lo dejará vacío, pues no es un elemento indispensable para el enrutamiento del mensaje. Añadirá el realm y host propio, la aplicación, es decir, el interfaz por donde se enrutará el mensaje y el código del comando, que para un Update Location Request es el 316.

Una vez tiene construido el mensaje, el MME mirará en su tabla de enrutamiento que debe hacer para encaminarlo. Como el realm de destino no coincide con su realm, debe enviarlo al agente Diameter que le indique su tabla de compañeros, que en este caso le indica, que debe enrutarlo al DEA de la red.

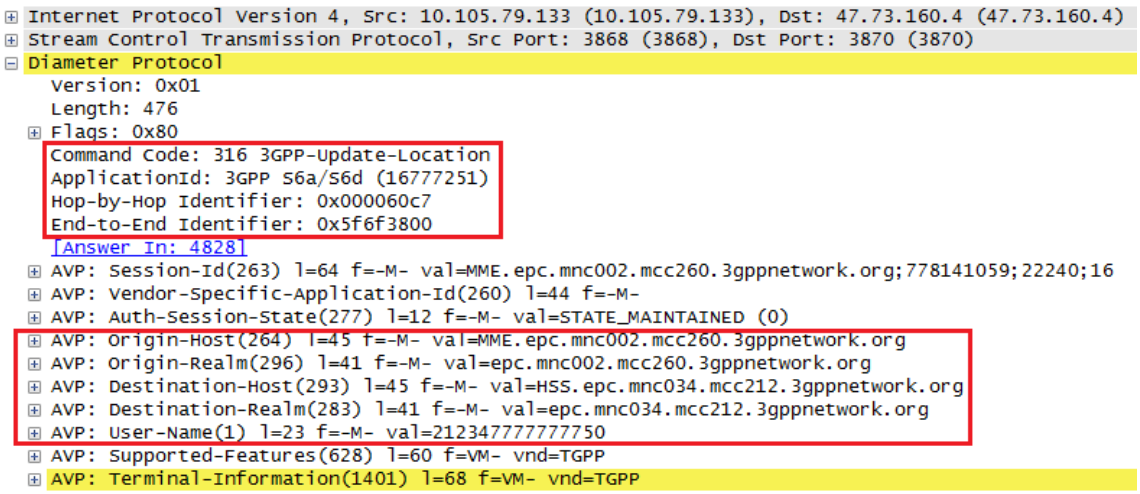

Figura 23: Traza de un registro de usuario en el entorno de laboratorio

El DEA de la operadora visitada recibe la petición por parte del MME y mira en su tabla de enrutamiento y tabla de compañeros, qué hacer con el mensaje, y cuál es el agente Diameter al que debe encaminarlo (pues el realm de destino no coincide con el suyo propio), obteniendo como resultado el DEA de la operadora local.

El mensaje ya se encuentra en el DEA de la operadora local y se repite el mismo proceso de chequear en la tabla de enrutamiento y de compañeros que hacer con el mensaje. Lo encamina al HSS.

El HSS que es el nodo Diameter que actúa como servidor en la sesión, al recibir la petición por parte de su DEA comprueba si existe información de subscripción para el IMSI indicado. Como el IMSI le es conocido, enviará un mensaje de respuesta al origen con un código de resultado satisfactorio, además del host y realm de origen, el identificador de la aplicación y el código de comando, que sigue siendo 316.

Como las respuestas a los mensajes Diameter son transaccionales, la respuesta es encaminada al origen atravesando los mismos agentes Diameter que atravesó en la petición, es decir, no es necesario aplicar ninguna lógica de enrutamiento. Con los AVPs de “End-to-End” y “Hop-to-Hop” la respuesta llega al nodo que originó el mensaje, que se trata del MME.

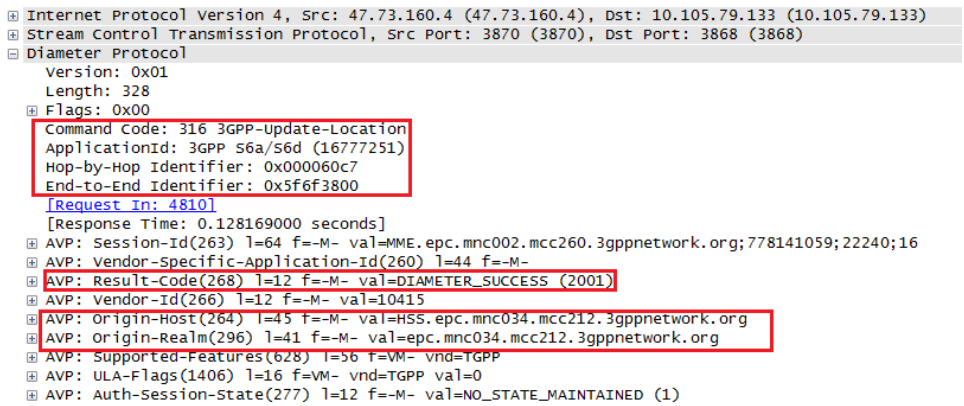

Figura 24: Respuesta a la petición de registro de usuario en el laboratorio

Capítulo 4

Centro de gestión de la itinerancia internacional (HUBs de roaming)

La itinerancia internacional se encuentra entre uno de los mayores éxitos de la GSMA. Los usuarios esperan tener acceso al mismo tipo de servicios independientemente de si están en su red local o se encuentran en el extranjero.

Los acuerdos bilaterales de itinerancia se convirtieron en uno de los factores limitantes para que ese éxito siguiera aumentando. La diversificación de servicios, el incremento de las tecnologías de acceso y la existencia de casi 800 operadoras miembros de la GSMA, hicieron temer que no se cumplieran las expectativas de los operadores de abrir nuevos acuerdos de itinerancia.

El coste total de la apertura de un acuerdo bilateral impidió que muchos operadores establecieran nuevos acuerdos de itinerancia, más si cabe cuando ya tenían un socio de itinerancia en el país deseado o cuando el volumen potencial de tráfico era bajo.

Con la introducción de nuevos servicios, el problema se hizo aún más evidente y el coste global mayor, ya que es necesario abrir un acuerdo bilateral para cada uno de ellos con el fin de asegurar que los usuarios serán capaces de utilizar dichos servicios en el extranjero. En Abril del año 2005, la GSMA anunció el lanzamiento del proyecto de “Conectividad Abierta” (OC, Open Connectivity) cuyos principales objetivos eran:

- Asegurar que los operadores serían capaces de permitir que sus clientes hicieran itinerancia internacional en cualquier otro operador miembro de la GSMA.

- Asegurar que los operadores 3GSM pudieran enviar y recibir servicios con otros operadores 3GSM e incluso con los que no lo son.

- Optimización de los costes asociados con el establecimiento y mantenimiento de los acuerdos de itinerancia internacional e interconexión.

Dicho proyecto englobó las siguientes líneas de trabajo:

- **"Centro de gestión de mensajes de texto y mensajes multimedia"**

Los centros de gestión o HUBs permiten la posibilidad de externalizar la interconexión de los servicios de mensajería de texto (SMS, short message service) y mensajería multimedia (MMS, multimedia message service) a un suministrador, que se encarga de la apertura de acuerdos y de la supervisión, mantenimiento y gestión de las incidencias que puedan surgir con otras operadoras.

La implantación de estos HUBs persiguió minimizar el esfuerzo dedicado en las operadoras para el lanzamiento y mantenimiento de estos servicios lo que propició un aumento en el número de acuerdos de interconexión.

La documentación sobre esta línea de trabajo está recogida en el documento IR.75 "Open Connectivity SMS Hubbing Architecture".

- **"Centro de gestión de itinerancia internacional"**

La ambición principal de los centros de gestión de itinerancia internacional o HUBs de roaming (término que utilizaremos a partir de ahora en el Proyecto Fin de Carrera) era la de reemplazar el establecimiento individual de los acuerdos de itinerancia internacional bilaterales por una estructura más eficiente y concentrada.

El documento de la GSMA que marca las directrices de los HUBs de roaming es el IR.80 "Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model" [11]. Los HUBs de roaming o SMS/MMS consiguieron a corto plazo mejorar la eficiencia del lanzamiento y mantenimiento de los acuerdos de itinerancia internacional e interconexión permitiendo incluso conectarse a un grupo grande de operadoras por menos coste de lo que suponía antes una apertura bilateral.

En las siguientes secciones del capítulo, haremos una descripción de lo que es un HUB de roaming, cuáles son los requisitos a alto nivel y a nivel técnico que deben cumplir y las distintas arquitecturas que se pueden implementar.

4.1 Objetivo

El objetivo de los HUBs de roaming es la simplificación del escenario de itinerancia internacional clásico, esquematizado en la figura 25, donde se muestra cómo cada operadora debe interactuar con el resto de operadoras para abrir acuerdos con cada una de ellas y para cada servicio.

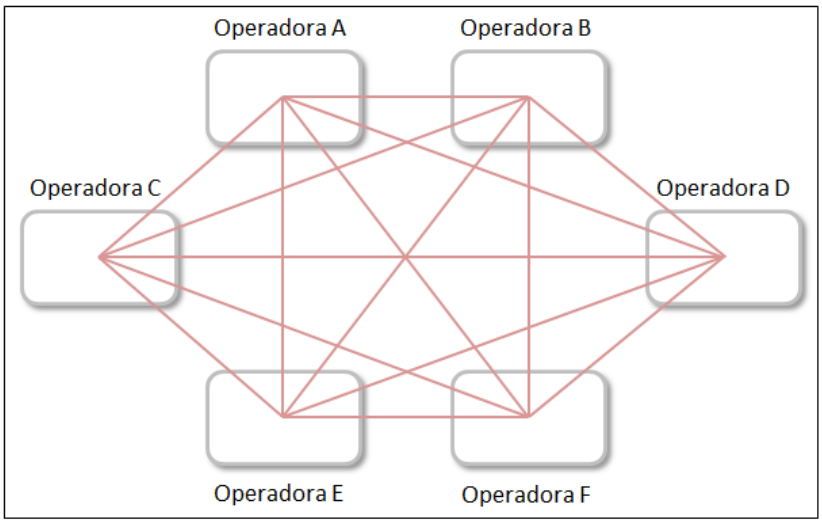

Figura 25: Escenario clásico de itinerancia internacional entre operadoras

El escenario fue reemplazado por una estructura más eficiente y concentrada, los HUBs de roaming, expuesto en la figura 26, que se encargan de todas las tareas asociadas a la apertura de los acuerdos, entre otras funciones, reduciendo al mínimo el esfuerzo que deben realizar las operadoras móviles.

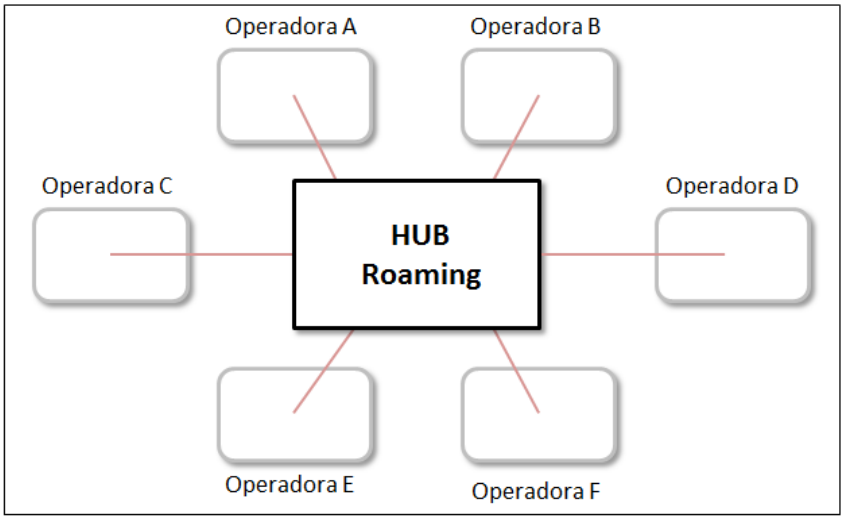

Figura 26: Escenario con HUB de roaming

Los HUBs de roaming centralizarán todas las comunicaciones y tareas asociadas al lanzamiento de los acuerdos comerciales entre las operadoras y otros HUBs de roaming. Se reduce de esta manera drásticamente el número de conexiones que posee cada operadora en el escenario general de la itinerancia internacional.

Además de la gestión de tráfico, los HUBs tienen la capacidad ofrecer otros servicios basados en los requisitos a alto nivel y requisitos técnicos desarrollados a continuación.

4.2 Requisitos a alto nivel

Detallaremos de forma muy breve los requisitos a alto nivel que deben cumplir los HUBs de roaming para ser compatibles con el estándar.

- **Solución abierta e interoperabilidad entre soluciones**: los proveedores de la solución deberán estar preparados para trabajar juntos y asegurar que las soluciones que ofrecen son totalmente compatibles e interoperables con el resto.

- **Obligación:** un operador puede tener una justificación regulatoria, estratégica o comercial para no establecer un acuerdo de itinerancia con otro operador. Cualquier solución empleada debe permitir a los operadores clientes del HUB elegir que acuerdos de itinerancia iniciar.

- **Transparencia**: El Hub debe:

    - Dar visibilidad de todos los componentes de precio impuesto.
    - Proveer al operador cliente información acerca de las redes que están originando y terminando el tráfico en él.
    - No manipular el contenido, formato o información relativa al tráfico transmitido a través de su solución.
    - Proporcionar al cliente toda la información necesaria para permitirle el análisis y solución de incidencias.

- **Eficiencia:** Se debe hacer uso eficiente de los recursos de red, minimizando cualquier gasto indirecto en la red visitada y en la red local. Se minimizará cualquier sobrecarga en la red visitada.

- **Calidad extremo a extremo:** debe comprometerse una calidad de servicio específica para la transmisión del tráfico extremo a extremo, que no se verá reducida por la inclusión de otros HUBs, proveedores de señalización u operadoras involucradas en la transmisión del tráfico. Además existirán mecanismos para medir el nivel de calidad conseguido.

    - El HUB de roaming ofrecerá al operador cliente un servicio completo y eficiente para la gestión de las incidencias y gestión del servicio.

- **Formación**: Se debe ofrecer soporte completo y formación a los clientes de la solución.

- **Fraude y seguridad:** la solución debe asegurar que los informes con la información de los usuarios en itinerancia, se hace manera correcta y en tiempo siguiendo los métodos de NRTRDE (Near Real Time Roaming Data Exchange).

- **Disponibilidad:** la solución debe asegurar una arquitectura altamente disponible, redundante y robusta, además de tener un plan de recuperación operacional en caso de desastre.

- **Pruebas:** la solución disminuirá al mínimo el tiempo y los recursos dedicados a las pruebas en los operadores implicados. Los HUB de roaming con capaces de realizar todas las pruebas extremo a extremo (end-to-end) descritas en la documentación correspondiente IREG y TADIG.

- **Agregación de contratos:** en el contrato con el cliente del HUB deben incluirse todas las operadoras móviles con las que desea tener acuerdo y para qué servicios.

- **Soporte de servicios y enabler:** el HUB deberá tener solución para las distintas necesidades que puedan surgir a nivel de interconexión o itinerancia.

- **Transparencia en los datos de itinerancia:** la solución garantizará transparencia en el destino de los clientes de una red local, de qué operadoras con los usuarios que acampan en una red visitada…

- **Tarificación en cascada**: el HUB gestionará las relaciones de tarificación y financieras de todos sus clientes y otros HUBs siguiendo el modelo en cascada del tráfico de voz.

- **Interconexión con otras soluciones:** será responsabilidad del HUB de la red local conectarse al HUB de la operadora visitada para garantizar la provisión de los servicios de itinerancia internacional entre ambas operadoras.

4.2.1 Requisitos técnicos

El grupo IREG creó un grupo de trabajo llamado "IREG Roaming Hub Group" con el objeto de definir los requisitos técnicos de los HUBs de roaming dentro del proyecto iniciado por la GSMA de conectividad abierta. Los principales requisitos técnicos son:

- **Centralización de la señalización**: la señalización para todos los socios de itinerancia internacional que no esté implementada de forma bilateral, será enrutada a través del HUB, reduciendo así la configuración de red en los operadores clientes.

- **Flujo de señalización en cascada**: el tráfico de señalización es retransmitido paso a paso por entidades intermedias siguiendo un flujo en cascada desde el origen al destino y viceversa. Existen dos posibilidades para el flujo de señalización:

    - A través de un túnel se transmite la señalización sin ninguna modificación entre origen y destino.
    - El flujo modifica la señalización para la transmisión entre el origen y destino.

- **Gestión de acuerdos**: antes de permitir el intercambio de señalización entre dos socios de itinerancia, el HUB debe verificar la relación contractual entre ambos.

- **Pruebas y monitorización de la calidad de servicio**: se trata de una función de valor añadido del HUB, a través de la cual asumen la responsabilidad de realizar

las pruebas IREG/TADIG en lugar del operador cliente. Adicionalmente, el HUB puede realizar pruebas periódicas y monitorización de los diferentes indicadores de rendimiento (KPI, Key Performance Indicator) y métricas de los diferentes servicios ofrecidos a los operadores cliente.

- **Mecanismos de prevención de fraude**: los mecanismos deben incluir las funcionalidades de NRTRDE (Near Real Time Roaming Data Exchange), HUR (High Usage Reports), aunque HUR ya no está soportado por la GSMA, "Anti-Spamming" (mensajes de texto basura) y "Anti spoofing".

- **Casa de compensación financiera (FCH, Financial Clearing House):** el HUB de roaming ofrecerá los servicios de compensación financiera y soporte al proceso de facturación entre operadoras al operador cliente.

- **Casa de compensación de datos (DCH, Data Clearing House):** no es obligatorio que los HUB de roaming ofrezcan dicha funcionalidad de transferencia de los ficheros de tarificación entre las operadoras al operador cliente, pero sí que necesitará tener visibilidad de dichos ficheros para el establecimiento de acuerdos comerciales con otros operadores.

- **Análisis y resolución de incidencias**: se debe ofrecer visibilidad del enrutamiento del tráfico de señalización para mejorar la investigación de las incidencias.

- **Coexistencia tecnológica**: si el HUB ofrece servicios en 2G/3G y 4G, todas las tecnologías deben coexistir en la misma infraestructura.

4.3 Arquitecturas

Antes de describir los distintos tipos de arquitectura existentes para la implementación de un HUB de roaming, debemos comentar una serie de aspectos que son comunes a todas las implementaciones.

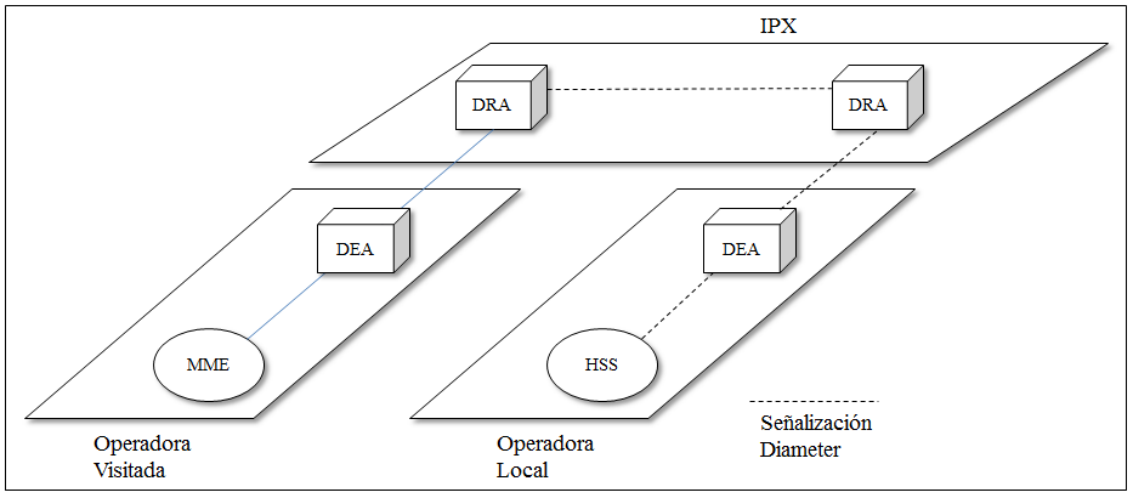

Figura 27: Escenario a alto nivel de la interconexión entre dos operadoras

En las arquitecturas de itinerancia internacional LTE clásicas, como la mostrada en la figura 27, el routing del tráfico de señalización Diameter entre la operadora visitada y la operadora local se realiza en base al realm, utilizando el mismo camino tanto en los mensajes de petición como en los de respuesta. Ambas operadoras suelen tener un DEA en la frontera de su red para poder esconder la topología de la misma a redes externas y se interconectan a la otra red a través de los DRAs del IPX.

Las operadoras deberán separar internamente el tráfico de señalización de los acuerdos bilaterales del que debe ser enviado a través del HUB de roaming. Dicha tarea también puede ser llevada a cabo por el carrier de señalización o IPX al que se encuentre conectado la operadora. En esto caso, el IPX deberá diferenciar el tráfico en función del realm de origen y el realm de destino.

4.3.1 Conexión directa

La operadora cliente deberá estar conectada directamente al HUB de roaming sin necesidad de utilizar un IPX para transitar la señalización. La señalización Diameter no es modificada en ningún momento.

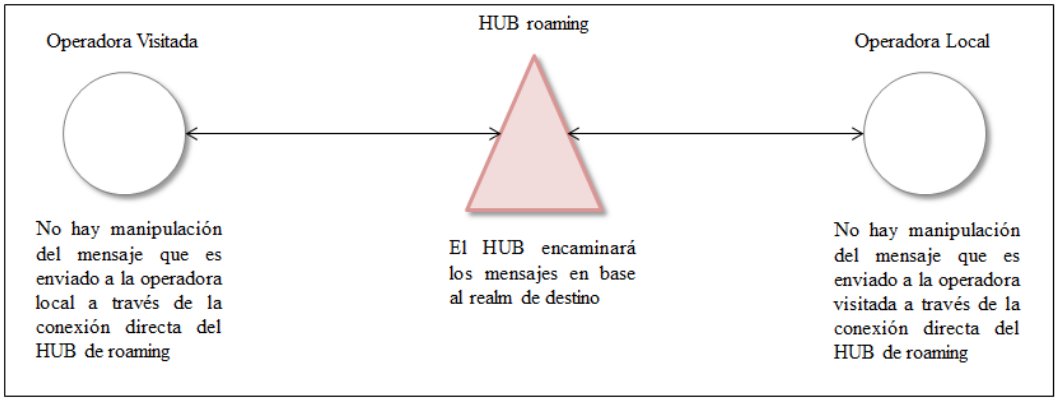

Figura 28: Conexión directa al HUB de roaming

El MME mandará el tráfico hacia el DEA de su red de acuerdo con las políticas de enrutado de tráfico y basándose en el realm de destino, es decir, el realm de la operadora local.

El DEA encaminará el tráfico hacia el DRA del HUB de roaming, dónde se chequeará si la combinación de realm de destino y host de destino coincide con alguna de las entradas de su tabla de enrutamiento y nodos adyacentes, si es así, reenviará el tráfico hacia el DEA de la operadora de destino.

El DEA de la operadora local, chequea el IMSI del tráfico recibido y si es conocido, lo reenvía hacia el HSS. El HSS aceptará o rechazará el ULR cambiando el realm y host de destino por el realm y host de origen, que en este caso, es el HSS.

4.3.2 Enrutado basado en realm de origen y destino

La operadora no está conectada directamente al HUB de roaming, así que necesitará de un proveedor de señalización (IPX) para poder enrutar el tráfico a la operadora de destino, es decir, la operadora local.

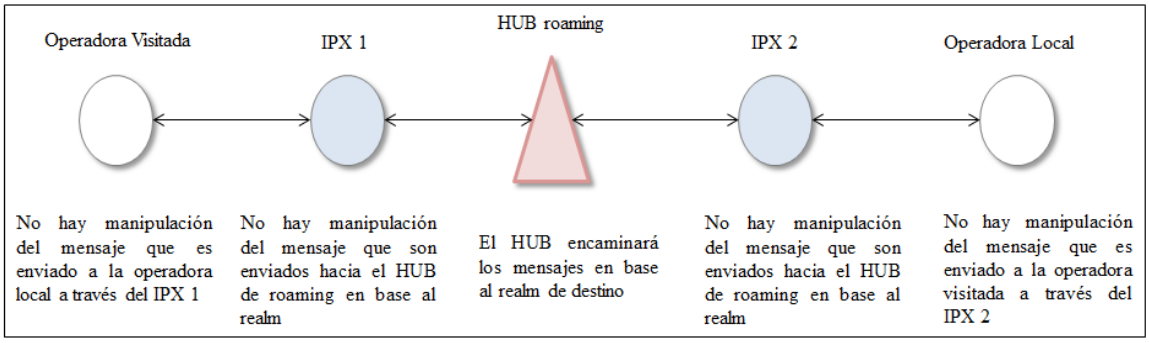

Figura 29: Enrutado basado en realm de origen y destino

El DRA localizado en el IPX, analizará el realm de origen y el realm de destino para saber dónde debe enrutar ese tráfico, pues podría encaminarlo a través del HUB de roaming o directamente a la operadora de destino si se tratara de acuerdo bilateral.

4.3.3 Modificación del realm de destino

La operadora tampoco está conectada directamente al HUB de roaming, así que como en la implementación anterior, hará uso de un IPX para encaminar el tráfico de señalización hacia la operadora de destino.

La particularidad que tiene este tipo de arquitectura, es que para enrutar el tráfico a través del HUB de roaming, es necesario añadir un realm propio identificativo del HUB al realm de destino.

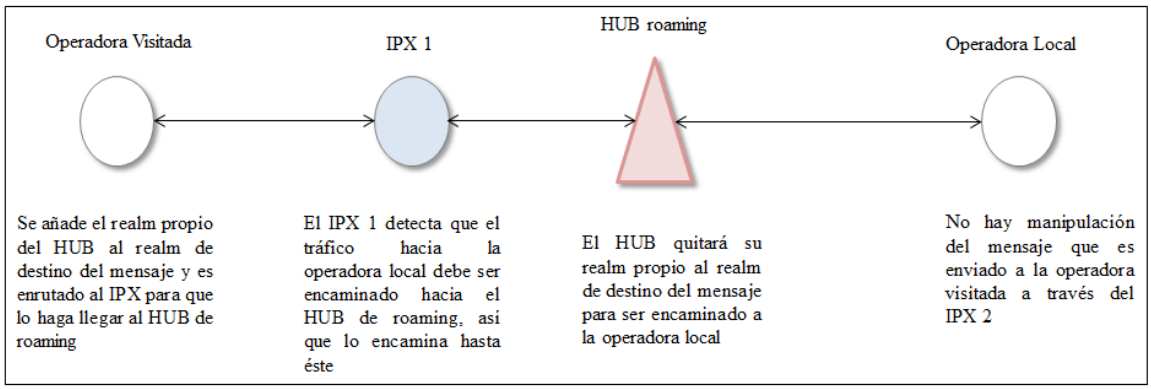

Figura 30: Modificación del realm del HUB de roaming

La operadora añadirá el realm propio del HUB de roaming al realm de destino, el IPX identificará el realm propio del HUB en el realm de destino del mensaje, así que lo encaminará hacia el HUB de roaming y éste tras comprobar el realm de destino y eliminar su realm propio, enrutará los mensajes hacia la operadora de destino.

Capítulo 5

Redirección del tráfico de itinerancia internacional

A pesar de vivir en una sociedad donde es difícil encontrar a alguien que no posea de al menos un teléfono móvil para poder acceder a todos los servicios proporcionados por las operadoras móviles, cuando viajamos al extranjero, muchos de nosotros decidimos apagar nuestros dispositivos móviles por el miedo a la factura.

La débil competencia entre las operadoras locales a la hora de prestar servicios a aquellos usuarios que se encuentran haciendo roaming en sus redes, ha provocado que los precios sean excesivos.

La comisión europea siempre ha puesto de manifiesto los altos costes del roaming dentro de la Unión Europea y ante la impasividad del sector de las operadoras móviles, en el año 2006 decidió intervenir en el mercado fijando unas tasas máximas para el servicio de telefonía, tanto para llamadas realizadas como para las recibidas, que las operadoras podrían cargar a los usuarios [12]. La regulación está siendo aplicada a todos los países miembros de la Unión Europea y a otros tres países que no forman parte de la Unión Europea, pero son parte del Área Económica de Europa.

Dicha regulación, conocida como la *"Euro tarifa"* fue aprobada por el Parlamento Europeo y el consejo de ministros y convertida en ley en el año 2007. Estos precios máximos fijados se debían aplicar a todos los clientes, salvo que su operadora de origen le ofrecieses una tarifa mejor y la fecha máxima de aplicación era el 30 de Junio del 2010. También se acordó informar a los clientes por medio de un mensaje de texto, de las

tasas por los servicios en roaming cuando se encontraban en el extranjero y se fijó un valor máximo a la factura que los usuarios podían recibir por parte de las operadoras.

En el año 2009, la ley fue enmendada para ampliar la fecha máxima de aplicación hasta el 30 de Junio del 2012 e incluir los mensajes de texto dentro de la regulación de precios, y a partir del año 2012, el tráfico de datos también fue regulado.

En la siguiente tabla podemos observar la disminución de precios para de los servicios anteriormente mencionados.

Año	Llamadas Originantes	Llamadas Terminantes	SMS originantes	SMS terminantes	Datos
2007	0,49€/min	0,24€/min	Sin regulación	Sin regulación	Sin regulación
2008	0,46€/min	0,22€/min	Sin regulación	Sin regulación	Sin regulación
2009	0,43€/min	0,19€/min	0,11 €	Gratis	Sin regulación
2010	0,39€/min	0,15€/min	0,11 €	Gratis	Sin regulación
2011	0,35€/min	0,11€/min	0,11 €	Gratis	Sin regulación
2012	0,29€/min	0,08€/min	0,09 €	Gratis	0,70€/MB
2013	0,24€/min	0,07€/min	0,08 €	Gratis	0,45€/MB
2014	0,19€/min	0,05€/min	0,06 €	Gratis	0,20€/MB

Tabla 3: Evolución precios itinerancia internacional

El 30 de Junio de este año 2015, las tres instituciones europeas (Comisión, Parlamento y Consejo) alcanzaron finalmente un acuerdo sobre el roaming que supondrá [13]:

- El fin se los sobrecostes del roaming en Europa a partir de Junio del 2017, es decir, utilizaremos nuestro teléfono móvil en la Unión Europea y pagaremos en función a la tarifa que tengamos contratada en nuestro país de origen.

- Para evitar abusos y prácticas conocidas como el *"Permanent Roaming"* (los abonados que compran en el extranjero una tarjeta USIM de la red móvil que desean y la utilizan cada vez que viajan a ese país, en lugar de utilizar su propia tarjeta USIM y hacer itinerancia internacional), se establecerá un límite de minutos, mensajes de texto y tráfico de datos por usuario. Si ese límite es superado, dichos servicios tendrán sobrecoste en la tarifa contratada.

- Con el fin de continuar con la bajada gradual de precios, se establece que a partir de Abril del 2016, los operadores solo podrán sumar 5 céntimos por llamada que realicemos desde otro país de la Unión Europea, 2 céntimos por los mensajes de texto y 5 céntimos por MB de datos consumido.

La itinerancia internacional o roaming contribuye de forma sustancial a los ingresos de las operadoras móviles, por ello, necesitan controlar de forma eficaz su negocio de roaming para que continúe siendo rentable. Sin embargo, puede ser una tarea complicada debido a dos razones principalmente:

- La operadora de la red local no es capaz de monitorizar de forma apropiada la calidad de servicio que se le está prestando a sus abonados cuando están

registrados en redes del extranjero ya que tiene muy poco control sobre ellos, lo que potencialmente puede provocar una mala experiencia de usuario.
- Los costes de la itinerancia internacional dependen de la red visitada y del acuerdo de roaming que se tenga con ella. Cuantos más usuarios haya registrados en las redes más caras, la rentabilidad disminuirá.

Dada la normativa europea sobre el roaming que está en vigor y que pondrá fin a los beneficios generados por el roaming en el año 2017, las operadoras deben ofrecer la mejor calidad de servicio a sus clientes en el extranjero reduciendo al máximo los costes generados de dicha actividad. Servicios como *"Steering Of Roaming"* tendrán como objetivo cumplir dicho fin.

5.1 ¿Qué es la redirección de tráfico de itinerancia internacional?

Cuando un usuario se encuentra en el extranjero, se realizará una selección de red, ya sea de forma manual o automática para poder registrarse en la red. Generalmente, existe más de una red que posee una cobertura radio adecuada y con la que nuestro operador tiene acuerdo de itinerancia. Sin embargo, no todas las redes son igual de provechosas para nosotros. Criterios como el área en el que se encuentra el usuario, el tipo de acuerdo de roaming firmado, los tipos de servicios ofrecidos o las características del terminal, harán que una de las redes sea más deseable y rentable que el resto.

La redirección del tráfico en itinerancia internacional o *"SoR"* (Steering of Roaming) por sus siglas en inglés, es un servicio desarrollado por las operadoras móviles para facilitar el registro de sus clientes en las redes visitadas que mayor beneficio pueden aportarle. Es un servicio ofrecido al usuario final y está focalizado en la reducción de costes y en mejorar la calidad de servicio [14].

La redirección del tráfico será realizada en base a dos criterios:

- **Comerciales**: centrados en disminuir el coste del servicio de itinerancia internacional para poder maximizar los ingresos de la operadora. Las redes con peor infraestructura o cobertura y con menos servicios disponibles, serán las redes más rentables a las que redirigir el tráfico de nuestros abonados.

- **Técnicos**: siempre enfocados a conseguir una alta calidad de servicio para que la experiencia del usuario sea satisfactoria utilizando la red con mejor infraestructura del país visitado.

Ambos criterios son incompatibles ya que para conseguir una calidad de servicio excelente será necesario redirigir los usuarios hacia las redes mejores que son normalmente las más caras. Las operadoras tendrán entonces que buscar un equilibrio entre ambos criterios para poder ofrecer un servicio de buena calidad al usuario final sin que los costes de itinerancia internacional se disparen.

La GSMA aprueba los sistemas redirectores de tráfico de itinerancia internacional entre las operadoras, promoviendo un uso razonable y responsable de estas técnicas para minimizar el perjuicio ocasionado a las redes visitadas y a los propios clientes. Sus recomendaciones quedan recogidas en las especificaciones IR.73 y BA.30.

5.2 Mecanismos de redirección

Los mecanismos que una operadora móvil puede utilizar para redirigir de forma efectiva a sus clientes hacia una u otra red son:

- La actualización de la tarjeta USIM de los usuarios.
- La manipulación de la señalización Diameter para las redes LTE (señalización ss7 para las redes 2G/3G).

Basándonos en estos mecanismos, podemos definir 3 estrategias a la hora de aplicar la redirección de tráfico:

- Redirección OTA (actualización de la SIM de usuario).
- Redirección mediante señalización (manipulación de la señalización Diameter).
- Redirección híbrida (manipulación de la señalización y actualización de la SIM).

Ambos mecanismos presentan ventajas e inconvenientes que serán descritas en las siguientes secciones, pero está demostrado que los mejores resultados son obtenidos cuando ambos mecanismos se aplican de forma conjunta.

5.2.1 Redirección OTA

La tecnología *OTA* (Over-The-Air) es utilizada en las comunicaciones móviles para modificar el contenido de las tarjetas UICC (más conocidas como tarjeta SIM o USIM) de los abonados de forma transparente al usuario mediante un SMS.

La redirección OTA es anterior a la existencia de los sistemas de redirección mediante señalización y se basa en la configuración de ciertos parámetros de la tarjeta USIM.

La tarjeta USIM mantiene registros internos de información de multitud de parámetros definidos por el usuario, el operador o la red. Dichos registros se denominan archivos esenciales y están definidos en la especificación 3GPP TS 31.102 [15]. De todos ellos, hay 2 que influyen directamente en la selección de red que realiza el terminal móvil:

- EFOPLMNwACT contiene la lista de redes preferidas y su tecnología de acceso en orden decreciente. El contenido es controlado por la operadora y puede ser modificado mediante actualización OTA.

- EFFPLMN contiene la lista de redes prohibidas. El contenido puede ser actualizado por la operadora o por el terminal.

La forma de actualizar las listas de redes preferidas o prohibidas una vez que la tarjeta USIM está en posesión del cliente es mediante el envío de mensajes OTA, que se encapsulan en un SMS y modifican el contenido de los registros EFOPLMNwACT y EFFPLMN.

El contenido de estos ficheros condiciona la selección de red que el terminal realiza en modo automático, ya que nunca intentará conectarse a una red prohibida, y siempre dará prioridad al registro en las redes preferidas.

A pesar de que la redirección basada en la OTA es mucho más efectiva que la redirección basada en señalización, el mecanismo tiene ciertas limitaciones:

- La nueva lista almacenada en la USIM no será actualizada hasta que el terminal reciba un comando de tipo “Refresh” o se apague y encienda de nuevo.

- Las redes móviles son elegidas siempre en el orden en el que aparecen en la USIM, por lo que no permiten fijar cuotas de tráfico que respalden los acuerdos comerciales, es decir, no podremos enviar el 70% de nuestro tráfico a la red A y el 30% restante a la red B. Además no permite hacer configuraciones personalizadas para cada usuario.

- La actualización para todo el parqué de tarjetas USIM de una operadora puede durar muchas semanas.

- La tarjeta USIM no tiene capacidad para almacenar las redes preferidas y prohibidas de todos los países. Por lo tanto suelen introducirse sólo las de los países que concentran la mayor parte del tráfico de itinerancia internacional de la operadora.

5.2.2 Redirección basada en señalización

Los sistemas de redirección basados en la señalización nacen de la necesidad de un sistema de redirección de tráfico más flexible que las plataformas OTA, como mecanismo para satisfacer los exigentes compromisos comerciales en itinerancia.

La redirección basada en señalización fuerza a los terminales móviles a registrarse en la red de nuestra elección, pues se rechazarán todo los intentos que se realicen en otras redes móviles. La redirección del tráfico se produce una vez el terminal ya ha realizado una selección de la red en la que desea registrarse, que como hemos dicho viene determinada principalmente por la configuración de la tarjeta USIM.

El sistema redirector se encontrará desplegado en la red del operador local o el HUB de roaming, en algún punto intermedio entre el DEA y el HSS, cuya función será interceptar y manipular los mensajes de señalización Diameter relacionados con la actualización de

la localización generados entre la red visitada y la red local del usuario, es decir, el mensaje Update Location Request (ULR).

Este método es el más extendido entre las operadoras móviles, pero no está exento de inconvenientes:

- Impacto en la experiencia del cliente ya que necesitará más tiempo para registrarse en las redes, y puede perder el servicio más a menudo debido a la redirección excesiva.

- Incremento del tráfico de señalización internacional. Se estima que el uso de este método de redirección aumenta los volúmenes de señalización entre la red visitada y la red local en torno a un 20% debido a los reintentos del terminal. La red local verá incrementado el coste de transmisión de este exceso de tráfico de señalización.

- Requiere mecanismos preventivos de control de tráfico ya que la redirección excesiva puede ocasionar congestión en las redes debido al incremento de señalización, especialmente en casos de incidencia o mantenimientos en la red, donde el tráfico de señalización puede incrementarse de forma exponencial.

5.2.3 Redirección híbrida

El mecanismo de redirección híbrida se basa en las ventajas de los mecanismos descritos hasta ahora, ya que las actualizaciones OTA son muy efectivas para garantizar que el terminal móvil se registre en la red preferida en el primer intento y la redirección basada en señalización es muy flexible.

La redirección híbrida asegurará que la tarjeta USIM del usuario posea la configuración apropiada para que el dispositivo móvil se intente registrar en la red preferida siempre que la cobertura sea buena. De esta manera, los casos en los que la plataforma de redirección tenga que rechazar intentos de registro por parte del abonado, se verán reducidos, provocando una mejor experiencia de cliente y menos costes para la operadora pues se reduce la señalización del tráfico internacional entre la operadora visitada y la local.

La plataforma OTA se conectará al sistema redirector tal y como se indica en la figura 31, y se encargará de enviar las actualizaciones OTA a los abonados en tiempo real.

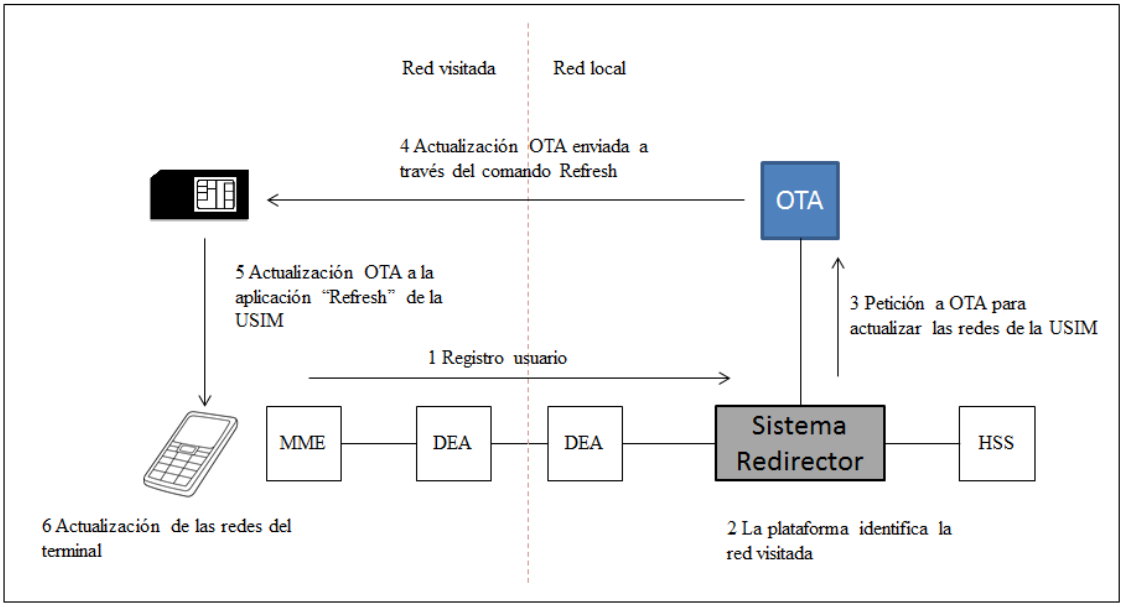

Figura 31: Esquema de redirección híbrida de tráfico de itinerancia internacional

A continuación, describimos cómo se produce la actualización OTA iniciada por la decisión de la plataforma de redirección:

1) El dispositivo móvil tras realizar el procedimiento de selección de red, lanza el intento de registro a la red.

2) La plataforma de redirección captura el mensaje de señalización y en función del realm de origen del mensaje puede identificar en que red visitada el terminal móvil está intentando registrarse.

3) Tras chequear la lista de redes preferidas y prohibidas para ese país, solicita a la plataforma de OTA que envíe ambas listas a la tarjeta USIM del usuario.

4) La comunicación son la USIM está cifrada, por lo que la plataforma OTA solicita a la operadora las claves de la USIM del usuario para poder construir el mensaje de actualización OTA, que será de tipo "Refresh" y será enviado al centro servidor de mensajería de texto de la operadora, encapsulado en un SMS.

5) El centro servidor se mensajes de texto entrega el SMS al abonado por los medios establecidos y terminal entrega la actualización OTA a la aplicación "Refresh" de la USIM.

6) La aplicación "Refresh" de la USIM actualiza la lista de redes del terminal, que realizará una nueva selección de red teniendo en cuenta las nuevas redes configuradas en su tarjeta.

Este mecanismo es totalmente transparente para el usuario pero es muy importante asegurar que la configuración de ambos sistemas es consistente para evitar resultados inesperados, es decir, que la plataforma de redirección fuerce el registro en una determinada red que en la USIM no está configurada como preferida.

5.3 Funcionamiento

Cada intento de registro en la red por parte de un usuario pasa por la plataforma o sistema de redirección de tráfico y ésta debe decidir si permite o rechaza el registro dependiendo del tipo de red visitada en la que se encuentre el usuario, es decir, red preferida, no preferida o prohibida. Cuando la plataforma recibe el intento de registro, debe chequear el realm de origen del mensaje de señalización para poder identificar la red visitada en la que el usuario está intentando registrarse. Recordemos que en el realm de los mensajes Diameter aparece el código del país (MCC) y el código de la red móvil (MNC), quedando de esta manera totalmente identificada la red móvil.

Una vez la plataforma de redirección de tráfico ha identificado la red visitada, tomará la decisión en base a la distribución de tráfico o preferencias que tenga configurada. Si la plataforma de redirección decide aceptar el intento registro, el mensaje es devuelto al DEA de la operadora para que sea transitado hacia el HSS tal y como ocurriría si no hubiese una plataforma de redirección entre ambas entidades de red. El HSS comprobará si existe información de subscripción para ese usuario y en función del resultado de la comprobación, enviará el mensaje de respuesta al MME.

En la siguiente figura podemos observar cómo se permite el registro del usuario en la red visitada.

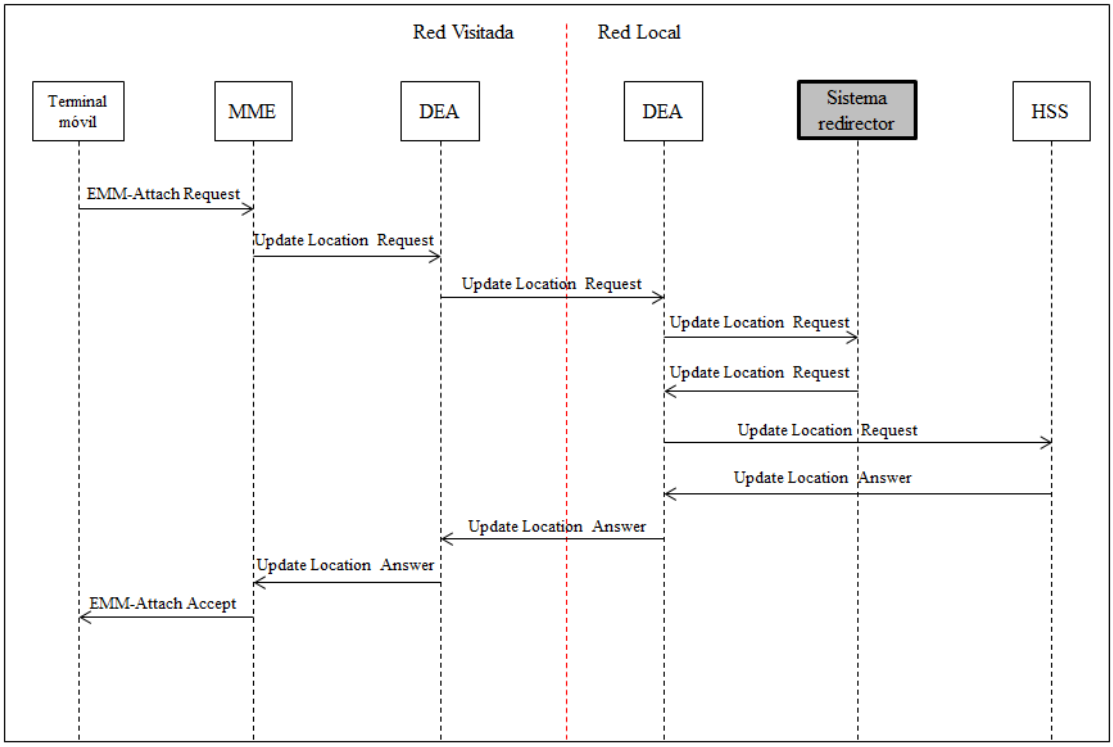

Figura 32: Sistema de redirección aceptando el registro en red del usuario

Si por el contrario, la plataforma de redirección de tráfico decide rechazar el intento de registro, generará el mensaje de respuesta con un código de error Diameter y lo enviará al DEA de la operadora para que sea transitado hacia el MME de la red visitada.

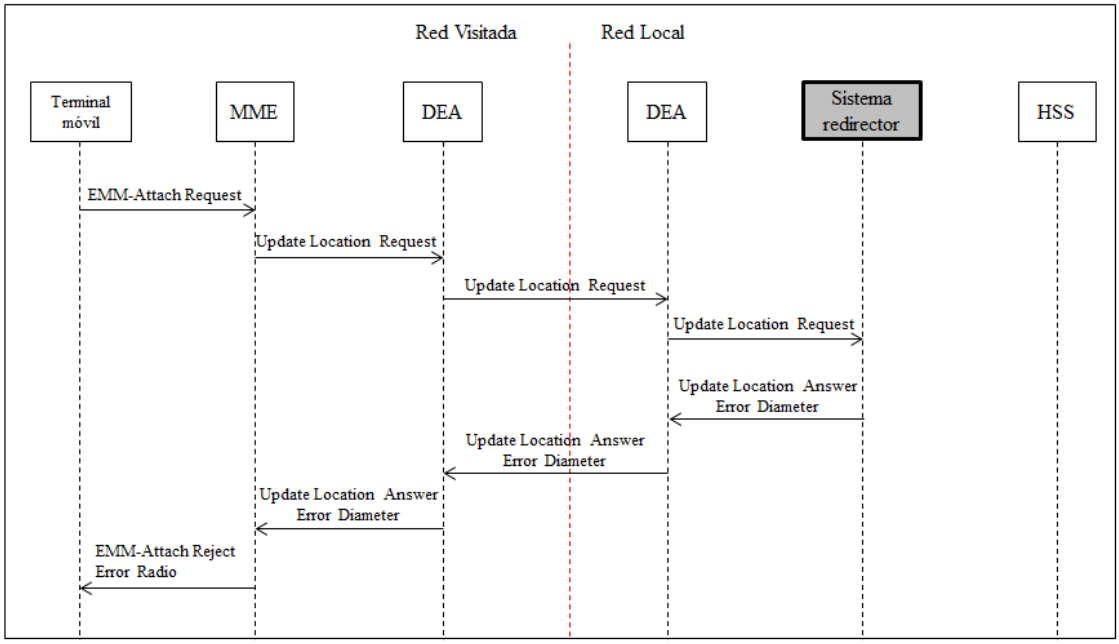

Figura 33: Sistema de redirección rechazando el intento de registro en red

Los rechazos por parte de la plataforma de redirección de tráfico simulan ser respuestas reales por parte del HSS de la red local al MME de la red visitada y según el código de error Diameter utilizado, el terminal móvil intentará registrarse de nuevo en la red o iniciará un proceso de selección de una nueva red.

Los códigos de error utilizados por parte de la plataforma pueden englobarse en dos grandes grupos:

- Códigos **no reintentables**: estos códigos de error provocan que el terminal móvil no vuelva a intentar registrarse en la red de la que acaba de ser rechazado.

- Códigos **reintentables**: estos códigos de error provocan que el terminal móvil pueda volver a intentar el registro en la red siempre y cuando cumpla una serie de requisitos que describiremos a lo largo de la sección.

Los códigos de error recomendados en el PRD de la GSMA IR.73 son:

Error Diameter	Código Error	Código Radio	Error Radio
DIAMETER_ERROR_ROAMING_NOT_ALLOWED, without Error Diagnostics	5004	#11	PLMN not allowed
DIAMETER_UNABLE_TO_COMPLY	5012	#17	Network Failure
DIAMETER_ERROR_ROAMING_NOT_ALLOWED, with Error Diagnostics of ODB_ALL_APN	5004	#19	ESM Failure

Tabla 4: Códigos de error recomendados para redirigir el tráfico

Aunque también pueden utilizarse cualquier código de error de la siguiente tabla:

Error Diameter	Código Error	Error Radio	Código Error
DIAMETER_ERROR_USER_UNKNOWN	5001	#8	EPS services and non-EPS services not allowed
DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION, without Error Diagnostics, or with Error Diagnostics of GPRS_DATA_SUBSCRIBED	5420	#15	Not suitable cells in tracking area
DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION, with Error Diagnostics of NO_GPRS_DATA_SUBSCRIBED	5420	#7	EPS services not allowed
DIAMETER_ERROR_RAT_NOT_ALLOWED	5421	#15	Not suitable cells in tracking area
DIAMETER_ERROR_RAT_NOT_ALLOWED	5421	#13	Roaming not allowed in this tracking area
DIAMETER_ERROR_RAT_NOT_ALLOWED	5421	#12	Tracking area not allowed
DIAMETER_ERROR_ROAMING_NOT_ALLOWED, with Error Diagnostics of ODB_HPLMN_APN or ODB_VPLMN_APN	5004	#14	EPS services not allowed in this PLMN
DIAMETER_AUTHORIZATION_REJECTED	5003	#15	Not suitable cells in tracking area
DIAMETER_UNABLE_TO_DELIVER	3002	#15	Not suitable cells in tracking area
DIAMETER_REALM_NOT_SERVED	3003	#15	Not suitable cells in tracking area
DIAMETER_INVALID_AVP_VALUE	5004	#17 o #42	Network Failure o Severe Network Failure
DIAMETER_AVP_UNSUPPORTED	5001	#17 o #42	Network Failure o Severe Network Failure
DIAMETER_MISSING_AVP	5005	#17 o #42	Network Failure o Severe Network Failure
DIAMETER_RESOURCES_EXCEEDED	5006	#17 o #42	Network Failure o Severe Network Failure
DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	5009	#17 o #42	Network Failure o Severe Network Failure
DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	4181	#17 o #42	Network Failure o Severe Network Failure

Tabla 5: Códigos de error Diameter

La operadora podrá utilizar cualquier otro código de resultado del protocolo Diameter no listado en las tablas anteriores, pero debe asegurarse que el código de error será traducido en el interfaz radio como “Network Failure”, es decir, error #17.

Antes de pasar a describir cada uno de los códigos de error recomendados por la GSMA, necesitamos conocer como el terminal móvil realiza la selección de la red y que contadores y temporizadores pueden influir en el comportamiento del terminal móvil cuando intenta registrarse en la red.

Comportamiento del dispositivo móvil

Los terminales móviles comprueban constantemente que están conectados a la red, si no lo están o la celda adyacente posee mejores niveles de señal, iniciarán el procedimiento de selección de red [16].

Si la selección se hace de forma manual por parte del usuario, deberá seleccionar entre todas las redes disponibles que se le muestran en la pantalla del dispositivo.

Sin embargo, si el procedimiento se realiza de forma automática por parte del terminal, éste intentará conectarse a la primera red disponible de las que tiene configuradas en la tarjeta USIM. La primera red a la que intentará conectarse es la red de la propia operadora, pero si nos encontramos en un escenario de itinerancia internacional, se elegirá la primera red disponible de las configuradas como redes preferidas, si dicha selección no es posible, se elegirá una de las no preferidas, pero nunca una red de las que se encuentran en el fichero de redes prohibidas de la tarjeta USIM. Si llegados a este punto no hemos conseguido conectarnos a ninguna de las redes configuradas en la tarjeta USIM, el terminal intentará conectarse a cualquier red no configurada para poder tener acceso al servicio.

Una vez el terminal móvil ha seleccionado la red, inicia el procedimiento de registro en la red, pero no siempre es exitoso, ya sea porque se está rechazando ese intento con un código de error reintentable o porque no hay respuesta por parte de la red. Con el fin de evitar que el terminal móvil esté continuamente intentando registrarse en la red, el dispositivo posee un contador interno que limitará el número de reintentos consecutivos en la misma red.

El contador de intentos fallidos de localización LTE se llama “Attach Attempt Counter” y su valor máximo es 5, es decir, si el quinto intento de registro en la red LTE es rechazado, el terminal móvil iniciará un nuevo proceso de selección de red entre las redes disponibles configuradas en su tarjeta USIM [17].

A parte del contador de intentos fallidos de localización, el terminal tiene definidos dos temporizadores que especifican por un lado el tiempo máximo de 15 segundos para recibir respuesta al intento de registro, T3410, y un tiempo de 10 segundos antes de iniciar el siguiente reintento, T3411, cuando no se ha recibido respuesta alguna. Cuando el terminal recibe un rechazo con código de error reintentable, el temporizador T3410 se para y si el número de reintentos realizados es inferior a 5, se procede a realizar un nuevo intento de registro tras 10 segundos como indica el temporizador T3411y se inicia el temporizador T3410 de nuevo. En el caso de que el número de reintentos fuera igual a 5, el terminal móvil iniciaría una nueva selección de red.

Pero si lo que ocurre es que el terminal no recibe respuesta al intento de registro, tras expirar el temporizador T3410, se esperarían los 10 segundos estipulados por el temporizado T3411 antes de reintentar el registro en red.

Ahora que ya conocemos el comportamiento del dispositivo móvil, vamos a describir que ocurre en cada uno de los casos en los que la plataforma de redirección del tráfico rechaza el registro y utiliza uno de los códigos de error recomendados por la GSMA.

1) DIAMETER_ERROR_ROAMING_NOT_ALLOWED, without Error Diagnostics (5004)

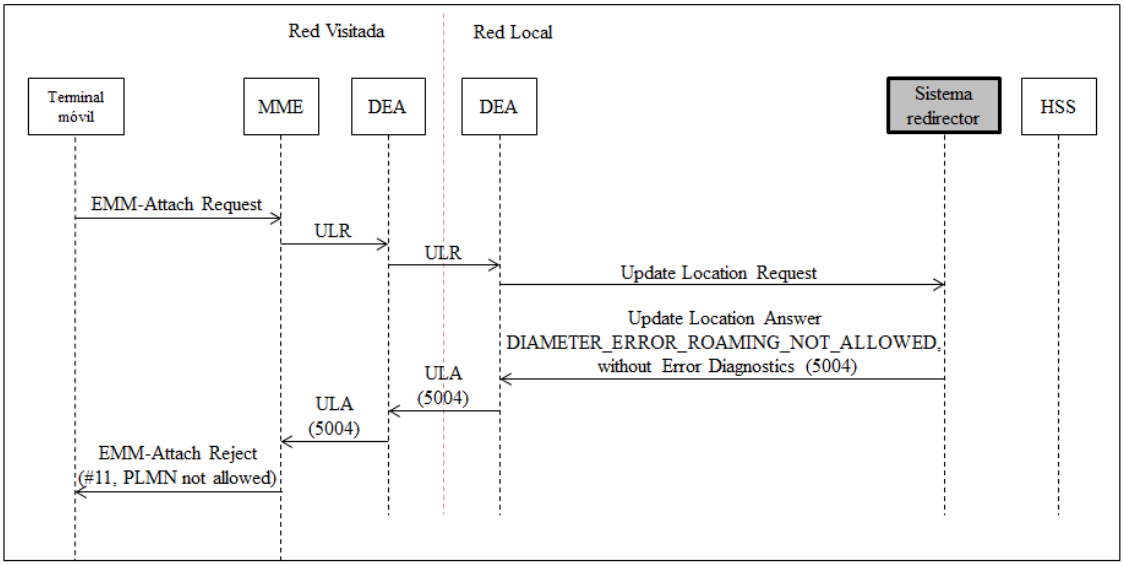

Figura 34: DIAMETER_ERROR_ROAMING_NOT_ALLOWED, without Error Diagnostics (5004)

Se trata de un código de error no reintentable que indica al dispositivo móvil que está intentando registrarse en una operadora visitada no permitida por su operador, así que el proceso de registro es rechazado y la red es incluida en la lista de redes prohibidas en la tarjeta USIM del usuario. El terminal deberá iniciar el procedimiento de selección de red para poder registrarse en otra red.

Dado que no se producen reintentos de registro en la red visitada, no se produce ningún aumento de la señalización Diameter entre ambas redes y la plataforma ha redirigido el tráfico en el primero intento, así que se trata de un código de error altamente eficaz desde el punto de vista técnico.

Pero se trata de un código de error muy agresivo porque su efecto es permanente salvo que el usuario intente conectarse a la red de forma manual o la operadora cambie la configuración de la lista de redes prohibidas en la tarjeta USIM mediante una actualización a través de la plataforma OTA.

2) DIAMETER_UNABLE_TO_COMPLY (5012)

Es un código de error reintentable que provocará que el dispositivo móvil intente registrarse hasta que el contador llegue a su tope, lo que provocaría el inicio del procedimiento de selección de una nueva red.

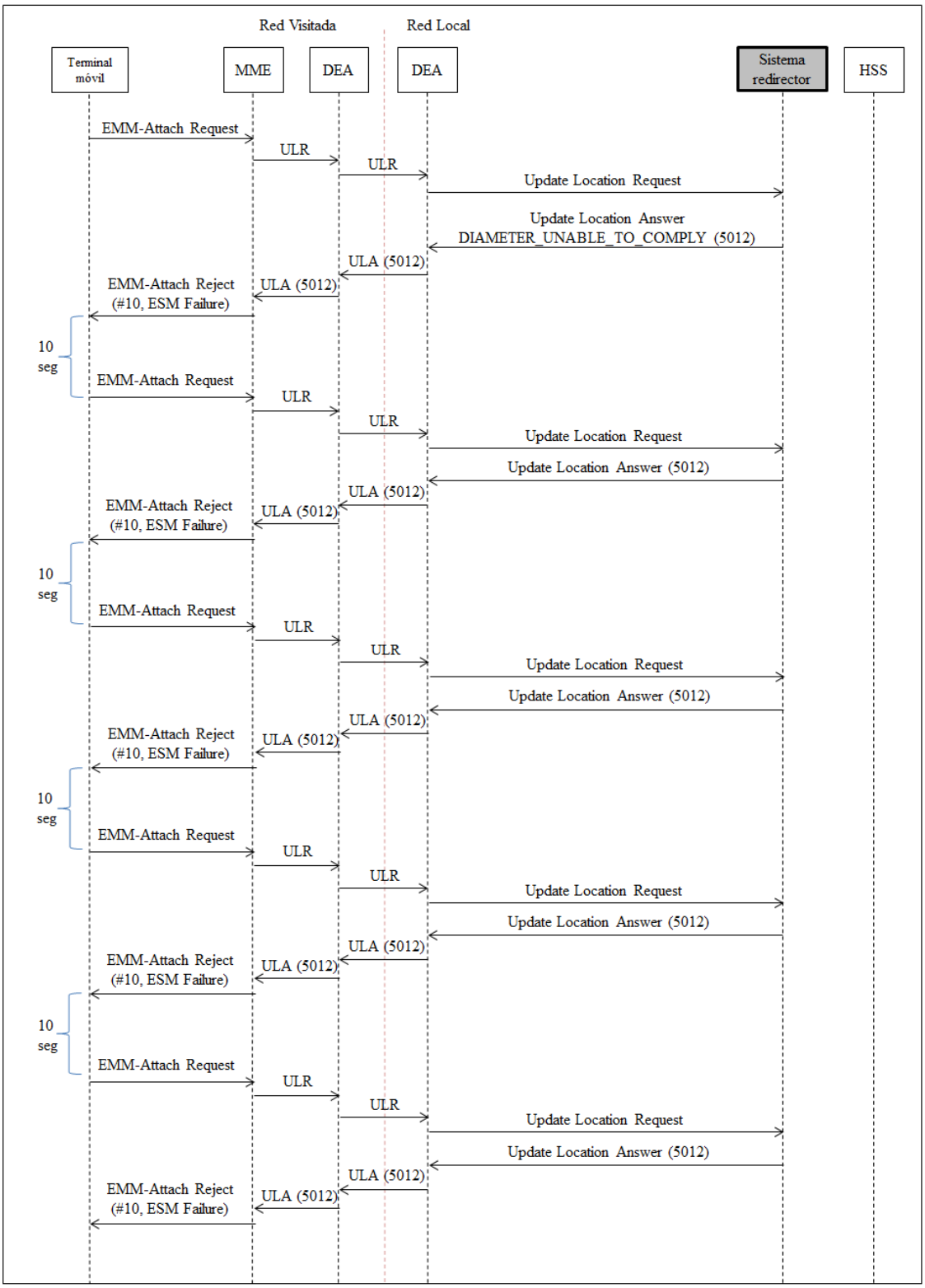

Figura 35: DIAMETER_UNABLE_TO_COMPLY (5012)

A los 10 segundos de recibir el rechazo por parte de la plataforma de redirección, se envía el nuevo reintento, hasta que al recibir el quinto rechazo, el dispositivo móvil buscará una nueva red en la que intentar registrarse.

Es una causa de rechazo poco efectiva técnicamente, pues se produce un aumento de señalización entre ambas redes y la redirección del tráfico no se produce hasta el quinto rechazo. Pero permitirá al usuario poder registrarse en la red más tarde pues la red no es incluida en la lista de redes prohibidas de la tarjeta USIM.

3) DIAMETER_ERROR_ROAMING_NOT_ALLOWED, with Error Diagnostic of OBD_ALL_APN (5004)

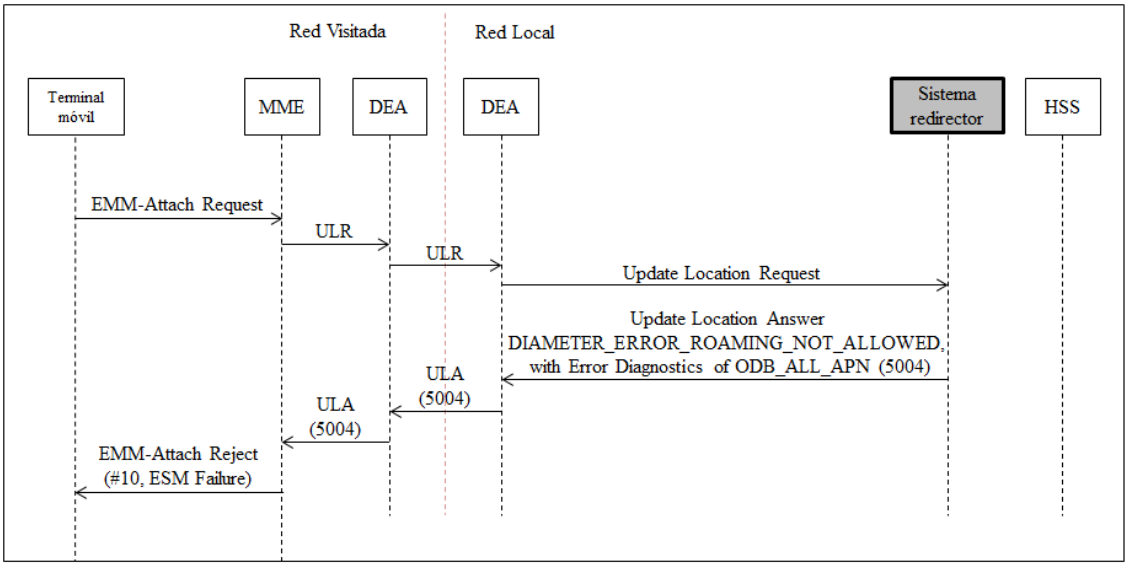

Figura 36: DIAMETER_ERROR_ROAMING_NOT_ALLOWED, with Error Diagnostics of OBD_ALL_APN (5004)

Se trata también de un código de error no reintentable, pues el terminal está intentando registrarse en una red no permitida por su operador, así que el dispositivo móvil deberá iniciar un nuevo procedimiento de selección de red. La diferencia con el código de error primeramente explicado, es que en este caso, la red visitada no es incluida en la lista de redes prohibidas de la tarjeta USIM del usuario, así que el dispositivo móvil podrá intentar utilizarla si fuera necesario, es decir, si no hubiese más redes disponibles.

Al igual que el primer código de error, se reduce la señalización entre ambas redes pues el terminal tras recibir el rechazo inicia el procedimiento de selección de red para registrarse en otra red. La redirección del tráfico se ha realizado de forma eficaz, tras el primer intento.

Sin embargo, dependeremos de la implementación LTE que se haya hecho en la red visitada, pues este código de error está disponible desde la versión 10 de la especificación LTE (actualmente nos encontramos en la versión 12), por lo que podría haber redes que no lo soporten. También debemos tener en cuenta, que la red visitada puede traducir de forma incorrecta el código de error en el interfaz radio, provocando comportamientos inesperados en el terminal.
Las redes locales, deben permitir a sus abonados poder conectarse de forma manual a las redes de las cuales han sido rechazados previamente.

5.3.1 CSFB: Circuit Switched Fallback

El concepto de CSFB introduce una gran complejidad en los escenarios en los que hay que aplicar redirección de tráfico. El registro combinado que se realiza en la red troncal EPC, tanto en el dominio de paquetes como para circuitos, debe ser redirigido de forma consistente para evitar que haya una interrupción del servicio proporcionado al usuario o causar problemas con la redirección del tráfico en el caso de que sólo el registro en uno de los dominios sea aceptado.

En la siguiente figura podemos observar cómo se realiza el registro del usuario en el dominio de circuitos y en el dominio de paquetes.

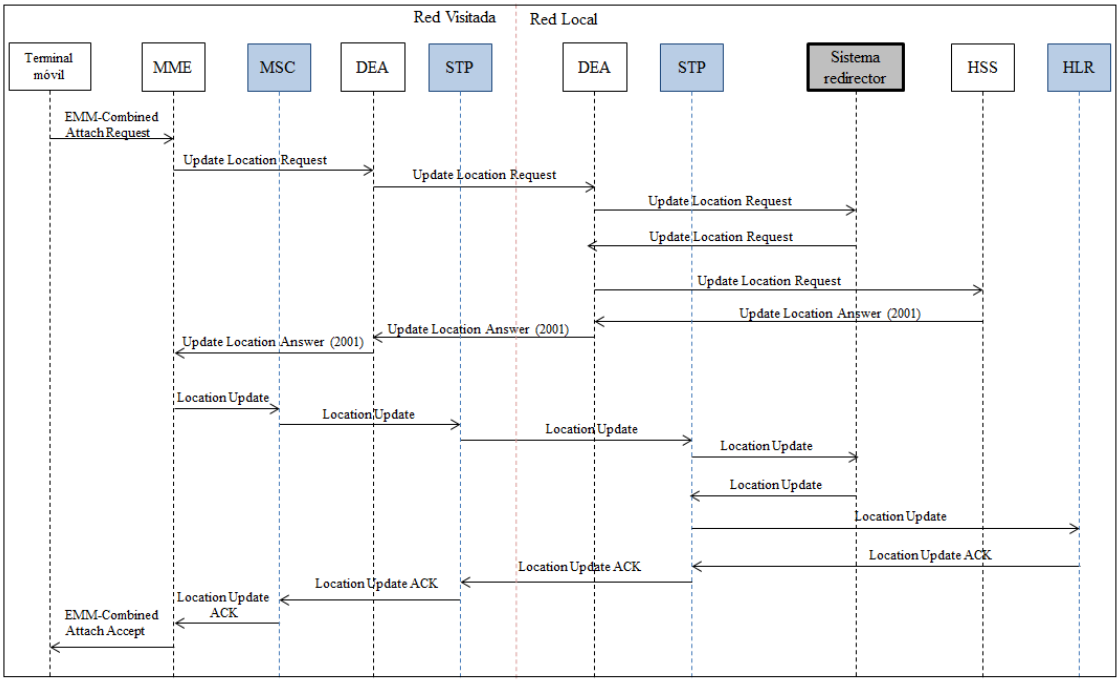

Figura 37: Registro en el dominio de circuitos y paquetes en un escenario con sistema de redirección de tráfico

Si por ejemplo, el registro en la red LTE se ha realizado de forma correcta, pero en la red 2G/3G no ha sido así por inconsistencia de la configuración del sistema redirector, dependiendo del terminal móvil podemos observar dos tipos de comportamiento diferente:

- **Voice Centric**: el terminal intentará el registro hasta que sea capaz de registrarse tanto en la red LTE como en 2G/3G. De acuerdo con la especificación de la GSMA, se reintentará un máximo de 5 veces para las redes LTE y GPRS, a diferencia del procedimiento GSM para los reintentos, que son un total de 4. Como el número de reintentos en LTE y GPRS es mayor que para GSM, la plataforma detectará de forma errónea que el usuario se está intentando registrar en la red de forma manual y permitirá el registro, pudiendo provocar que el usuario no sea redirigido en la red 2G/3G cuando lo debería haber sido en función de la red LTE en la que se encuentra registrado.

- **Data Centric**: el terminal intentará registrarse pero si en el quinto intento es rechazado, continuará registrado en la red LTE y dejará de intentar registrarse en el dominio de circuitos.

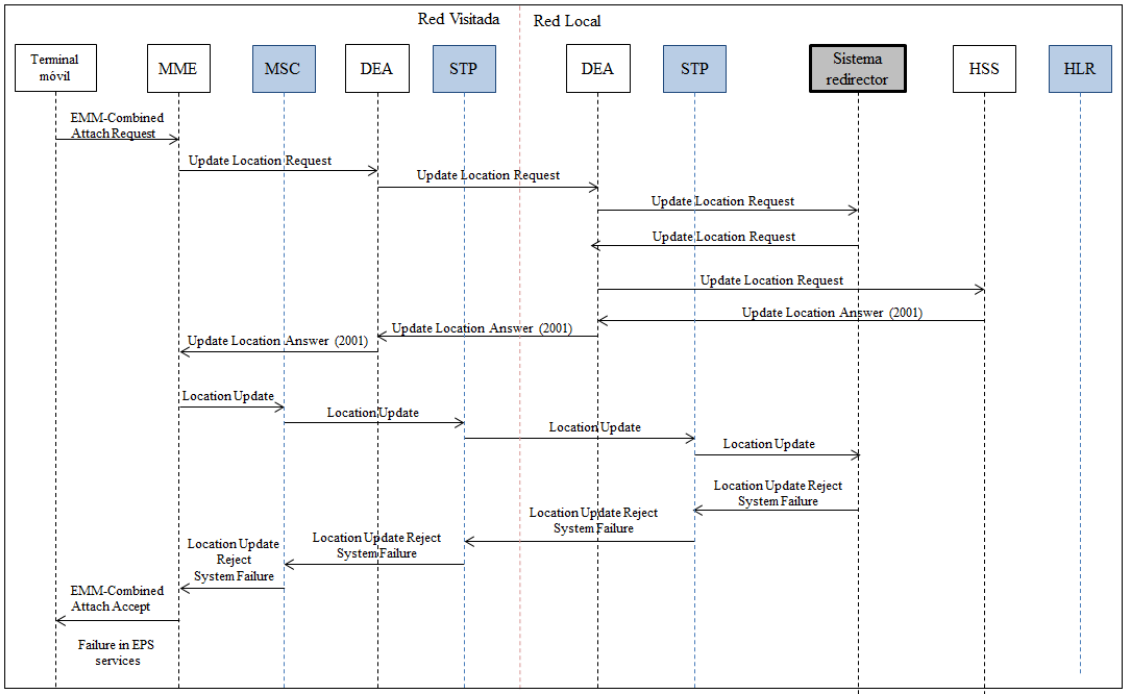

Figura 38: Escenario de CSFB con redirección de tráfico inconsistente

5.4 Directrices de implementación GSMA

Como hemos comentado en la segunda sección de este capítulo, la redirección mediante la manipulación de la señalización es un método que puede tener un efecto negativo sobre las operadoras y abonados. Por ello, la GSMA ha definido una serie de recomendaciones y buenas prácticas a la hora de implementar estos sistemas [18].

5.4 Requisitos implementación para la red local

- La redirección de tráfico se realizará sobre el protocolo Diameter.

- La redirección se aplicará solamente a los mensajes utilizados en los procedimientos de localización, es decir, el ULR y nunca en los empleados durante el proceso de autentificación.

- El sistema redirector sólo enviará una respuesta por procedimiento de actualización de la localización.

- En caso de encontrarnos en un escenario de CSFB, dónde existen mensajes para el procedimiento de localización en el dominio de circuitos y paquetes, los mensajes de señalización deberán ser redirigidos de forma consistente.

- Utilización de códigos recomendados en la especificación.

- Detección de selección manual de red por parte del usuario:

    - Permitir el segundo intento de registro en la misma red cuando se ha utilizado un código de rechazo no reintentable y que no configura la red como prohibida en la tarjeta USIM del usuario.
    - Permitir el sexto intento de registro en la misma red cuando se utilizan códigos de rechazo reintentables.

- El sistema redirector puede utilizar un realm específico para rechazar el intento de registro. De ser así, se deberá informar debidamente a las redes visitadas de forma proactiva o bajo demanda, para simplificar la identificación de errores debidos a la redirección de tráfico frente a errores de red reales.

5.4.2 Requisitos de implementación para la red visitada

- No se debe interferir en los procedimientos de registro iniciados por los usuarios.

- La respuesta a los intentos de registro debe trasmitirse de forma transparente hasta el dispositivo móvil sin ser manipuladas.

- No se deben generar intentos de registro falsos, es decir, aquellos que no se generan debido al procedimiento de actualización de la locación de un terminal móvil.

- No descartará el tráfico proveniente de un realm específico utilizado para el sistema redirector de tráfico.

Capítulo 6

Análisis y estudio del sistema redirector de tráfico

Ahora que ya hemos enmarcado este proyecto fin de carrera dentro del ámbito de las telecomunicaciones y más concretamente en el mundo de la itinerancia internacional, estamos preparados para adentrarnos en el objetivo del proyecto, que es el estudio y el despliegue de un sistema de redirección de tráfico en las redes LTE. Básicos son los conocimientos adquiridos en los capítulos anteriores para entender y estudiar la funcionalidad de dichas plataformas de redirección de tráfico.

A lo largo del capítulo, se estudiarán varios escenarios de itinerancia internacional antes y después de introducir el sistema redirector de tráfico, revisando si los objetivos comerciales y compromisos de calidad de servicio se cumplen tras aplicar la redirección. Además se revisarán los requisitos, los problemas encontrados y soluciones propuestas durante el plan de despliegue e implantación del sistema redirector de tráfico tanto en el entorno de laboratorio como en el entorno de tráfico real.

6.1 Casos bajo estudio

En esta sección describiremos como se realizará el análisis del sistema redirector de tráfico desde un punto de vista técnico. Para ello, se enunciarán los casos que se estudiarán antes y después de la aplicación de la redirección al tráfico y que indicadores

utilizaremos para evaluar su efectividad así como el impacto de la calidad de servicio percibida por los clientes en las configuraciones de redirección más clásicas.

Tendremos los siguientes escenarios que se estudiarán antes y después del despliegue del sistema redirector en la red:

1) **En el país visitado tenemos tres redes móviles, denominadas operadora A, operadora B y operadora C.**

   Previa a la redirección del tráfico, los usuarios se registrarán libremente en una de las tres redes móviles posibles en base a las redes que se encuentren preconfiguradas en su tarjeta USIM.

   Una vez la plataforma esté redirigiendo el tráfico, la operadora A será la red preferida, la operadora B será la red no preferida y la operadora C será la red prohibida.

2) **En el país visitado existen tres redes móviles, denominadas operadora D, operadora E y operadora F.**

   Al igual que en el caso anterior, los usuarios se registrarán en una de las redes móviles en base a las preferencias configuradas en su tarjeta USIM.

   La operadora D será configurada como la red no preferida, la operadora E como la red preferida y la operadora F también como red no preferida en el sistema de redirección de tráfico.

3) **En el país visitado existen tres redes móviles denominadas operadora G, operadora H y operadora I.**

   Las operadoras G y H se configurarán como redes prohibidas en el sistema redirector, mientras que la operadora I será la red preferida.

Estudiaremos un escenario dónde el cambio al dominio de circuitos (CSFB) esté presente también. No debemos olvidar, que la redirección del tráfico en este tipo de escenarios ha de realizarse de forma consistente para evitar al usuario la pérdida del servicio. Este escenario será desarrollado en la sección dónde se describen las pruebas funcionales que se realizaron en el entorno de laboratorio.

En el estudio de los casos se realizará un estudio comparativo de los datos estadísticos obtenidos por el sistema redirector de tráfico antes y después de la activación de la redirección. La recopilación de datos se hará a lo largo de 14 días y se mostrará el valor medio en las gráficas de análisis.

Como hemos visto en los casos descritos antes, la configuración está basada en un país con 3 redes móviles disponibles y cada una de ellas podrá ser configurada como red preferida, red no preferida o red prohibida. Dependiendo de los requisitos comerciales impuestos por la operadora de la red local.

El código de rechazo utilizado por el redirector será uno de los enunciados a lo largo del capítulo anterior. En las próximas secciones de este capítulo se definirán los códigos de rechazo utilizados.

Utilizaremos dos indicadores para realizar la comparativa entre los resultados obtenidos antes y después de aplicar la redirección al tráfico:

Distribución de usuarios

Este indicador representa el porcentaje de intentos de registro que el sistema redirector ha permitido en cada red, para un país visitado dado. Compararemos este valor con las preferencias configuradas en la plataforma para observar cuanto se ha desviado del objetivo marcado. Es calculado en base a un período de tiempo dado, que en nuestro caso será de 14 días. Es el número de registros permitidos por el sistema redirector en la red X, dividido por la suma del número de registros que han sido permitidos para todas las redes del mismo país bajo estudio.

$$Distribución\ usuarios\ Red\ X\ (\%) = \frac{Nº\ registros\ aceptados\ en\ red\ X}{\sum Nº\ Registros\ aceptados\ (Red\ X + Red\ Y + Red\ Z)}$$

Tiempo de registro

Representa el tiempo que necesita un usuario para registrarse en alguna red del país visitado cuando es sometido a redirección. Es calculado como el tiempo que transcurre desde el primer intento de registro de un abonado que es redirigido por la plataforma de redirección hasta que el intento de registro en el país es aceptado por el sistema redirector.

Para poder medir el tiempo de registro, que está relacionado de forma directa con la calidad de servicio percibida por el usuario, se han definido una serie de umbrales que facilitarán el estudio.

Umbral	Tiempo (segundos)	Calidad de servicio
T0	0	Excelente
T0 - T1	0 - 80	Buena
T1 - T2	81 - 160	Aceptable
T2 – T3	161 - 180	Mediocre
> T3	> 180	Deficiente

Tabla 6: Umbrales de tiempo de registro en red

Los umbrales están definidos en función al comportamiento que esperamos que tenga el dispositivo móvil en base a las especificaciones técnicas. El umbral T0 está definido para cuando el terminal se conecta directamente en la primera red que lo ha intentado, es decir, no ha habido redirección del tráfico en ningún momento, bien porque la red en la que ha intentado conectarse es una red preferida para su operador o porque no existe ninguna plataforma que se encargue de redirigir el tráfico.

Aunque en las redes LTE el número máximo de registros es 5 y son realizados cada 10 segundos, tenemos que tener en cuenta el escenario en el que el terminal móvil va al dominio de circuitos. En las redes 2G/3G el número máximo de reintentos es 4 para las redes GSM y 5 intentos para las redes GPRS y éstos se realizan cada 20 segundos. Si la causa de rechazo de la plataforma de redirección es reintentable, el usuario necesitará al menos de 80 segundos para intentar conectarse a nueva red tras haber sido rechazado de una previamente.

El umbral T3 está configurado a 180 segundos, que sería el tiempo máximo que permitiríamos al usuario estar intentando registrarse en alguna de las redes disponibles, basándonos en el caso bajo estudio, es decir, un país visitado con 3 redes móviles disponibles. Si llegados a ese valor el terminal continúa intentando registrarse en la red, el cuál ha sido redirigido ya 3 veces, en el siguiente reintento que realice, será aceptado por la plataforma de redirección independientemente de la red en la que se encuentre. Sin embargo, este temporizador no se aplicará para los intentos de registro que provengan de una red prohibida. En ese caso, el sistema redirector de tráfico continuará rechazando el tráfico.

6.2 Migración tráfico saliente (outbound) de la operadora

Un requisito básico para poder ofrecer el servicio de redirección del tráfico de itinerancia internacional a una operadora móvil, es que todo su tráfico de señalización esté centralizado, ya sea a través de un único proveedor de señalización (IPX) o un HUB de roaming.

Normalmente las operadoras móviles utilizan más de un proveedor para transitar el tráfico de señalización internacional, para evitar que el servicio se vea afectado o interrumpido en el caso de que uno de los proveedores tenga una incidencia.

Sin embargo, tal y como hemos explicado en el capítulo de los HUBs de roaming, son muchos los beneficios de centralizar la señalización en una única infraestructura, que además se encargará de la gestión de los acuerdos de itinerancia, pruebas extremo a extremo o investigación y resolución de incidencias entra muchas más tareas.

El escenario del que partimos está representado en la siguiente figura.

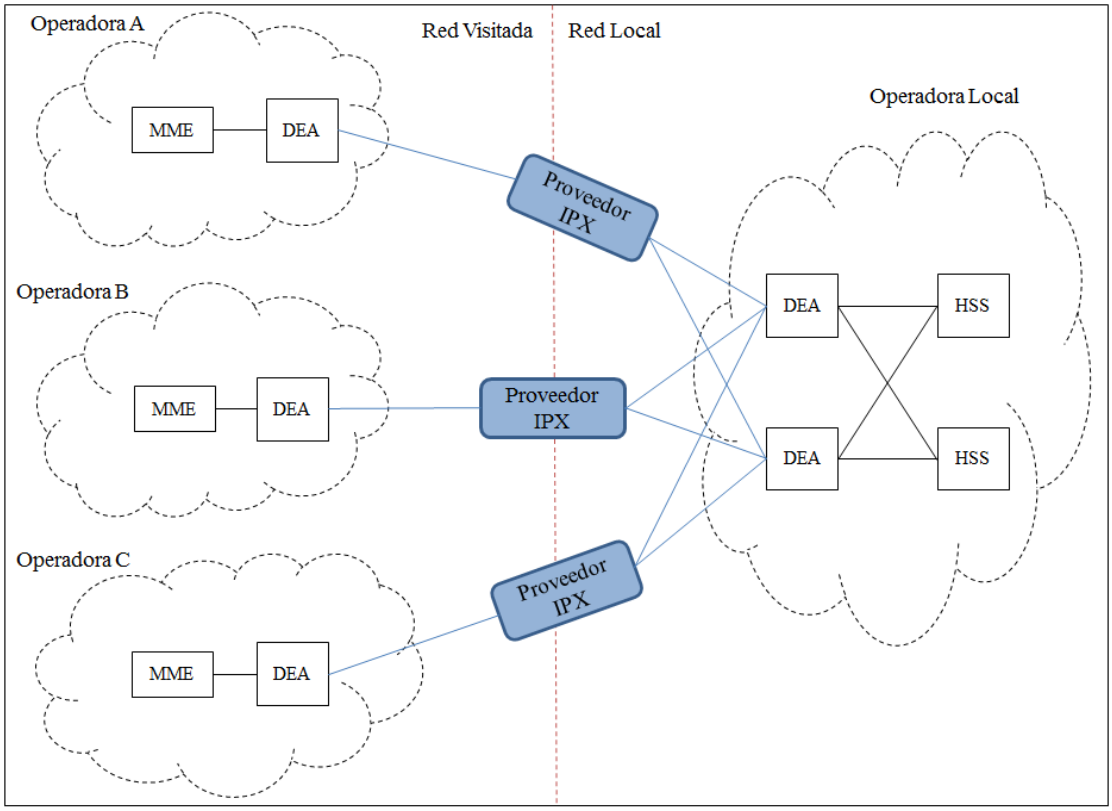

Figura 39: Escenario clásico de itinerancia internacional

La operadora móvil utiliza diferentes proveedores de señalización para transitar el tráfico hasta sus socios de itinerancia. Para poder centralizar todo su tráfico, se interconectará de forma directa con el HUB de roaming y el tráfico será migrado a la infraestructura, dando como resultado el escenario de la siguiente figura:

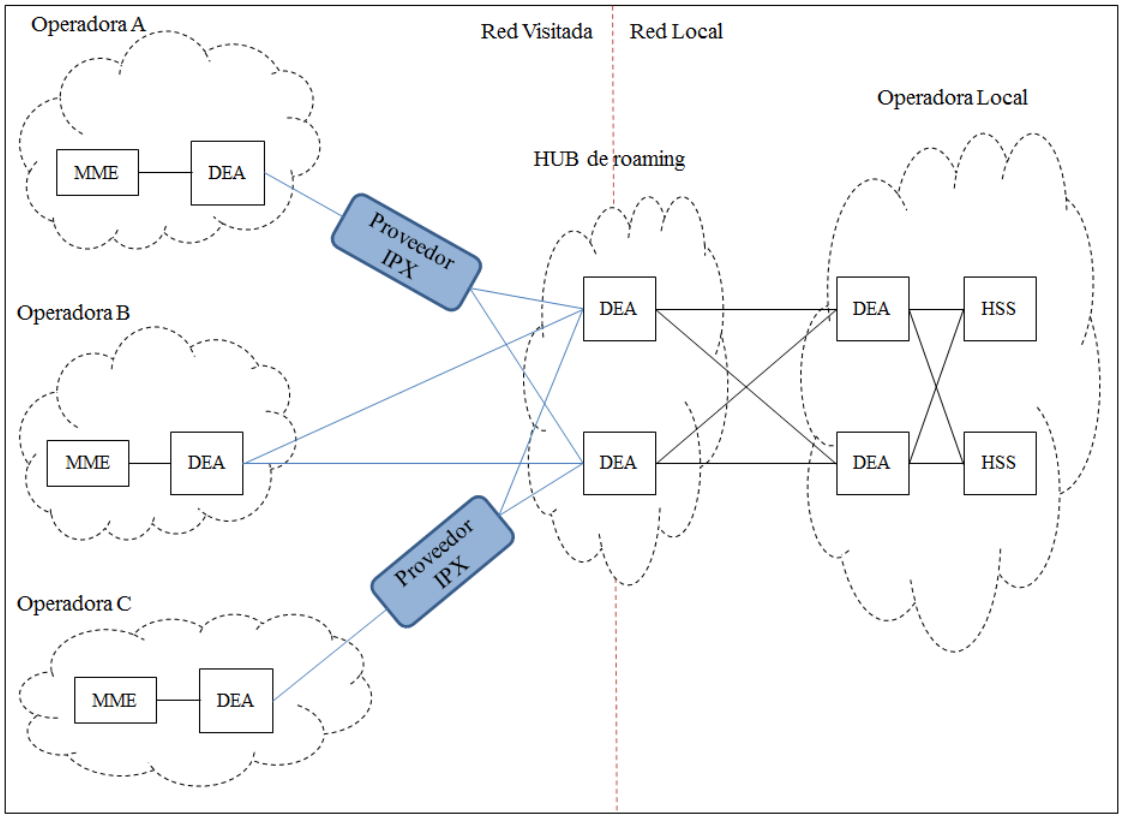

Figura 40: Escenario de itinerancia internacional con HUB de roaming

A continuación detallamos cada una de las fases:

1- Conexión directa entre la operadora y el HUB de roaming

Los departamentos de Ingeniería de red se pondrán en contacto para hacer el diseño de la conexión física y lógica. La interconexión entre la red IP de la operadora y del HUB de roaming se realizará a través de un par de puntos de presencia física (PoPs, Points of Presence) por cada una de las partes, localizados en centros de conmutación lo más cercanos posibles de la infraestructura del HUB de roaming, para asegurar la redundancia física de la interconexión.

La redundancia lógica será conseguida a partir de la creación de dos caminos de red diferenciados a nivel de capa de transporte diseñados a través de conexiones IP/MPLS (MultiProtocol Label Switching). Se utilizará el protocolo BGP (Border Gateway Protocol) para intercambiar la información de encaminamiento entre ambas redes.

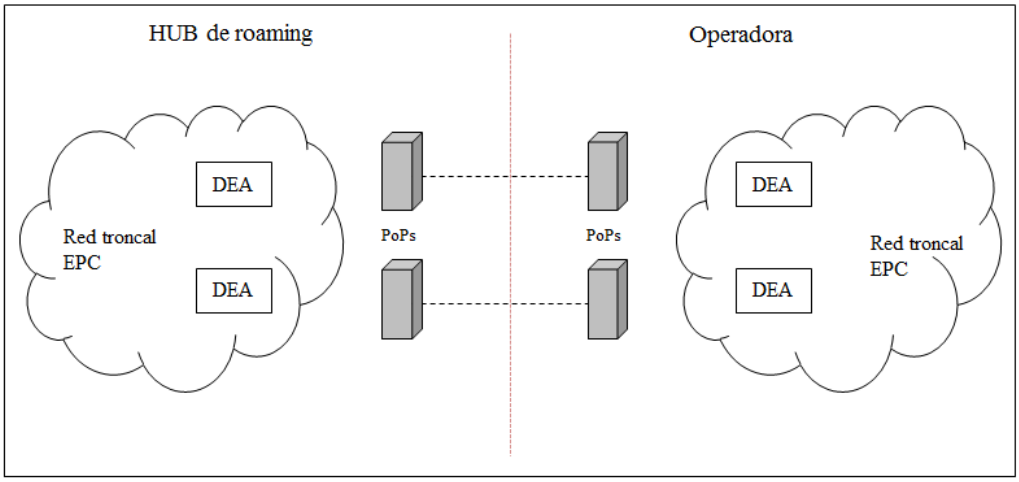

Figura 41: Interconexión física y lógica entre HUB de roaming y operadora

En paralelo, se realizará el diseño de la conexión Diameter entre los DEAs de la operadora y los DEAs del HUB de roaming. Normalmente, las operadoras, proveedores de señalización o HUBs de roaming poseen de al menos dos DEAs en su red. El diseño estará basado en el protocolo de señalización Diameter, protocolo en el que está basado el interfaz S6a y que utiliza el protocolo SCTP (Stream Control Transport Protocol) para la capa de transporte.

2- Configuración de las entidades de red

Mientras la interconexión entre ambas redes está en proceso de implementación, la operadora deberá proveer al HUB de roaming con la lista de operadoras visitadas con las que tiene acuerdo de itinerancia internacional, el documento IR.21 (documento técnico de la operadora que contiene información básica sobre sus elementos de red, rango de IMSI, realm, etc.) de cada una de ellas y el proveedor de señalización que utilizan para encaminar el tráfico.

Código TADIG	País	Nombre Operadora	IMSI	realm	Proveedor de señalización
ITAWI	Italia	Wind	22288	epc.mnc088.mcc222.3gppnetwork.org	IPX 1
GBRCN	Gran Bretaña	O2	23410	epc.mnc010.mcc234.3gppnetwork.org	IPX 2
POLKM	Polonia	Polkomtel	26001	epc.mnc001.mcc260.3gppnetwork.org	IPX 3
USACG	Puerto Rico	AT&T	310410	epc.mnc410.mcc310.3gppnetwork.org	IPX 1
USAW6	Estados Unidos	T-Mobile	310260	epc.mnc260.mcc310.3gppnetwork.org	IPX 2
DEUD1	Alemania	T-Mobile	26201	epc.mnc001.mcc262.3gppnetwork.org	IPX 2
NORTM	Noruega	Telenor	47900	epc.mnc000.mcc479.3gppnetwork.org	IPX 3

Tabla 7: Documento de control con las operadoras a migrar

Una vez recopilada toda la información en un mismo documento, podremos identificar los cambios que han de realizarse en las entidades de red del HUB de roaming. Los proveedores de señalización de la operadora también deberán realizar cambios de

configuración en su red para encaminar el tráfico de la operadora a través del HUB de roaming. Informaremos a los proveedores de señalización, las fechas en las que está previsto realizar la migración de tráfico para que los cambios se hagan de forma coordinada.

3- Planificación, migración y monitorización del tráfico

Una vez la interconexión IP está implementada y la conexión Diameter está en servicio entre los DEAs del HUB de roaming y de la operadora, estaremos preparados para comenzar a migrar todo el tráfico de itinerancia internacional de la operadora a través de la infraestructura centralizada.

Dependiendo de la cantidad de acuerdos de itinerancia internacional que posea la operadora, la migración de tráfico será realizada a lo largo de varias semanas. En la primera semana se migrará y monitorizará el tráfico de una única relación de itinerancia para certificar que la conexión está perfectamente configurada. En las siguientes semanas, se migrarán grupos de relaciones de itinerancia hasta que todo el tráfico esté migrado al HUB de roaming.

6.3 Análisis de los escenarios previos a la redirección del tráfico

Una vez todo el tráfico de itinerancia internacional de la operadora está centralizado, podemos realizar un primer estudio y análisis de los escenarios previos a la redirección del tráfico.

Escenario 1: país visitado con tres redes móviles denominadas operadora A, operadora B y operadora C.

Los usuarios se conectarán a las redes que tengan configuradas en la lista de redes preferidas de su tarjeta USIM y si éstas no están disponibles, continuarán con la lista de redes no preferidas, dejando para última instancia redes no configuradas en la USIM pero con buena potencia de señal.

En la siguiente gráfica, podemos observar la distribución de usuarios entre las 3 operadoras del caso de estudio.

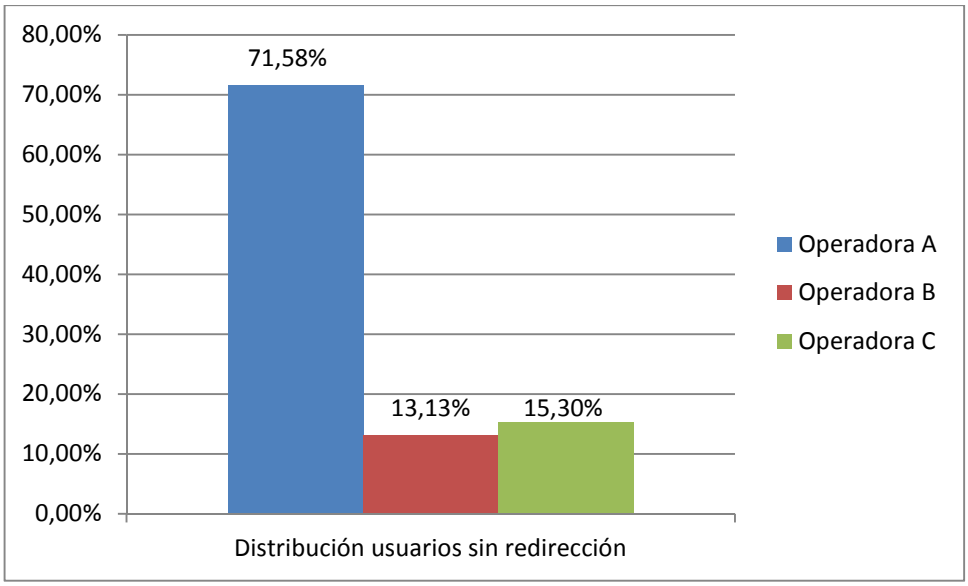

Figura 42: Distribución de usuarios en escenario 1 previa la redirección

Casi el 72% de los usuarios se han registrado en la operadora A, mientras que el 28% restante se ha dividido entre la operadora B y C en valores muy similares.

Por los datos obtenidos, podemos deducir que la operadora A es la que posee mejor cobertura móvil y mejor infraestructura de red dentro del grupo de operadoras del país, ya que la mayor parte de los usuarios se han registrado en ella. Normalmente las redes con mejor infraestructura y cobertura móvil son aquellas que nos van a reportar menores beneficios pues la tarifa entre las operadoras será más cara.

Como no estamos aplicando redirección al tráfico, el usuario se conecta en la primera red en la que intenta registrarse, lo que se traduce en una calidad de servicio excelente pues puede acceder a los servicios ofrecidos por la red desde el primer momento.

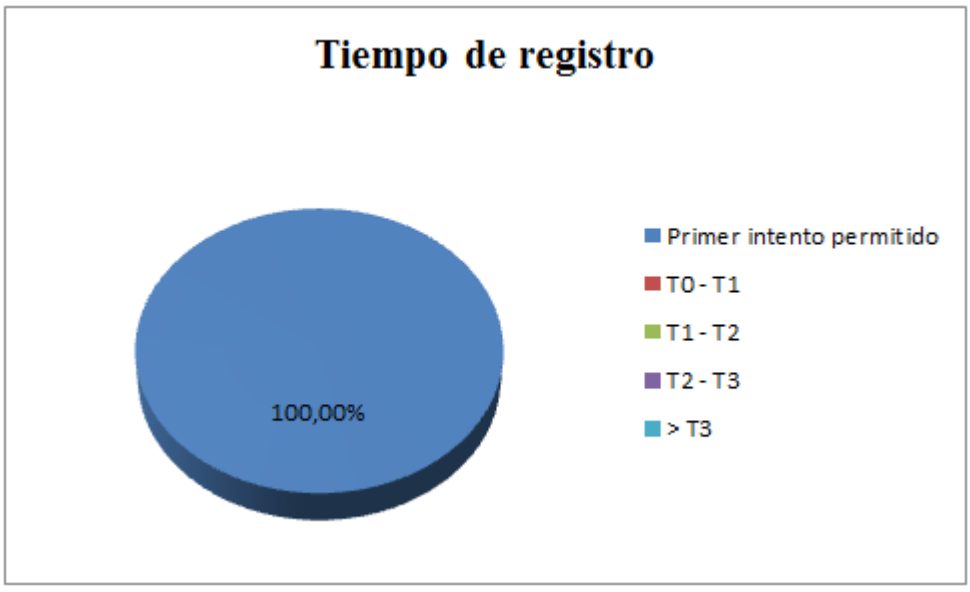

Figura 43: Tiempo de registro escenario 1 previo a la redirección

Escenario 2: país visitado con tres redes móviles denominadas operadora D, operadora E y operadora F.

Al igual que en el escenario anterior, los usuarios se registrarán en función de las redes preferidas que tengan configuradas en su tarjeta USIM. La distribución de usuarios que se observa en este escenario es el siguiente:

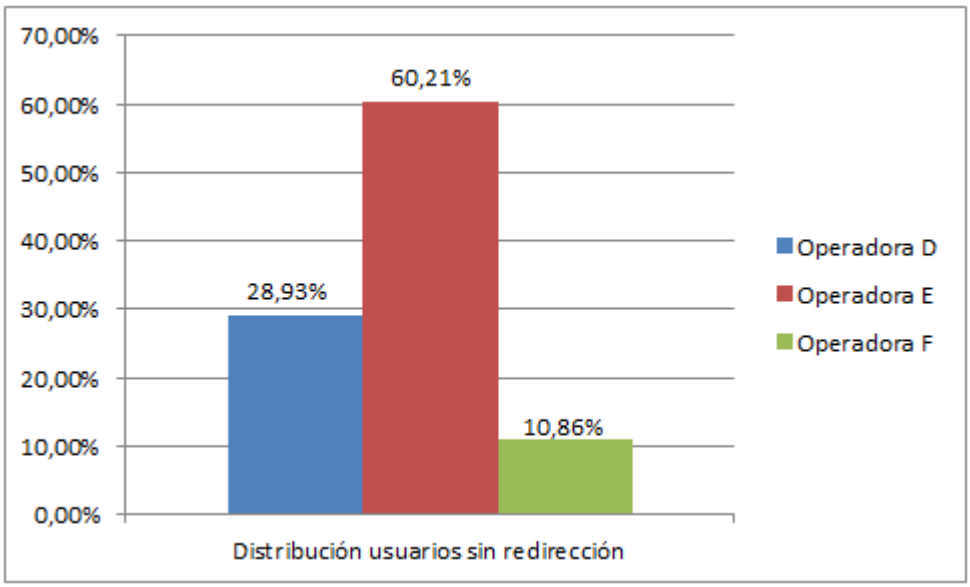

Figura 44: Distribución de usuarios en escenario 2 previa a la redirección

La mayor parte de los usuarios, en torno al 90% de ellos consigue registrarse en las redes de las operadoras D y E y el resto lo hacen en la red del operador F. En este escenario no podemos asumir que exista una red claramente con una buena infraestructura o buena cobertura en todo el país, pues los usuarios se distribuyen a lo largo de dos operadoras principalmente.

Al igual que en el caso anterior, los usuarios se registran en las distintas redes existentes en el país en el primer intento y por lo tanto, no existirá ningún tiempo de espera para poder acceder a los servicios que ofrece la red.

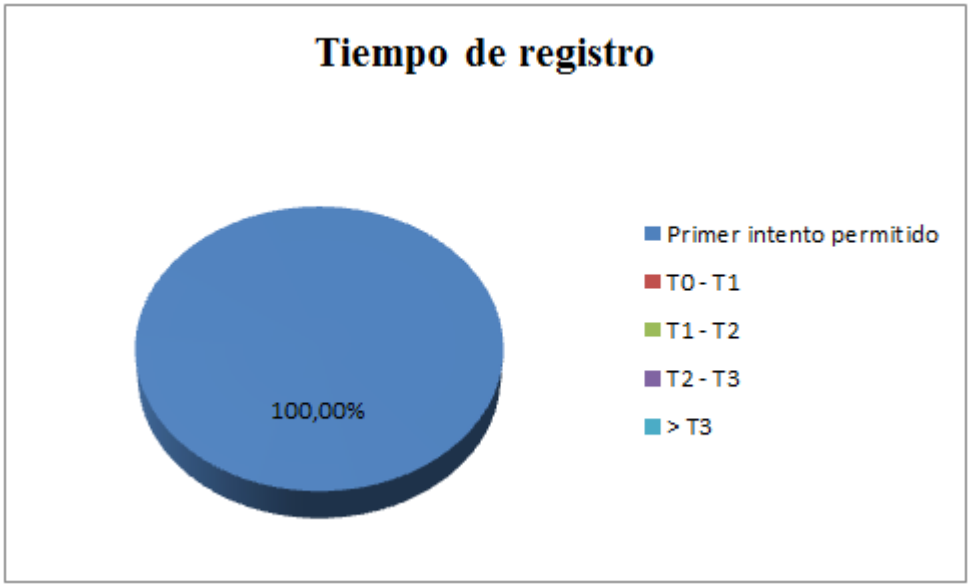

Figura 45: Tiempo de registro escenario 2 previo a la redirección

Escenario 3: país visitado con tres redes móviles denominadas operadora G, operadora H y operadora I.

En este escenario volvemos a tener tres operadoras en el país visitado, en el que los usuarios se conectarán a la red configurada en su tarjeta USIM. En la siguiente figura podemos observar la distribución de los usuarios en este caso.

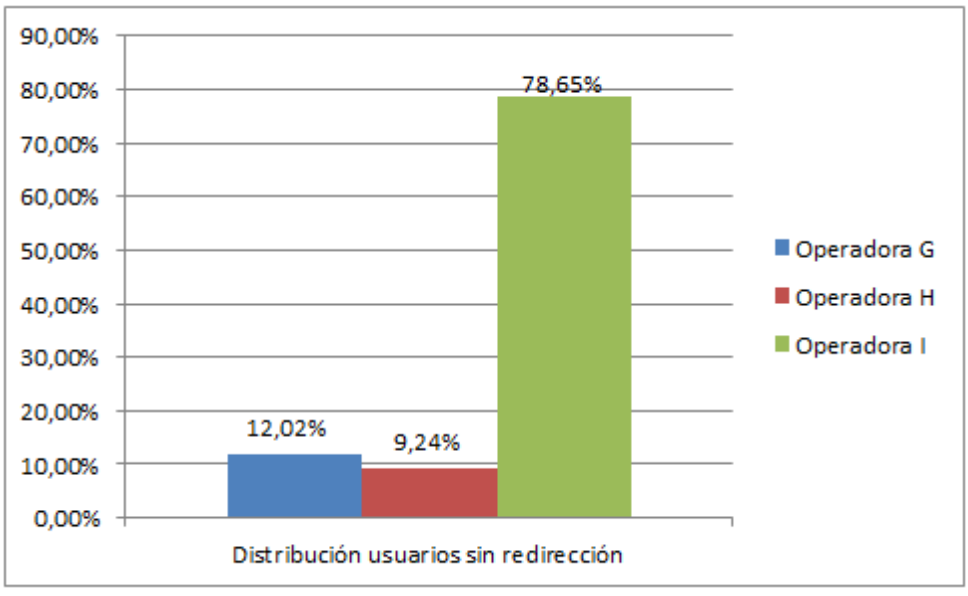

Figura 46: Distribución de usuarios en escenario 3 previa a la redirección

Parece claro que la red móvil con mejor cobertura en el país y seguramente también con la mejor infraestructura es la localizada en la operadora I. Los usuarios se registraran en el primero intento ya que no hemos activado aún la redirección del tráfico. En la siguiente

figura mostramos el conocido gráfico circular dónde se ilustra que el usuario consigue registrarse en la red en el primer intento de registro.

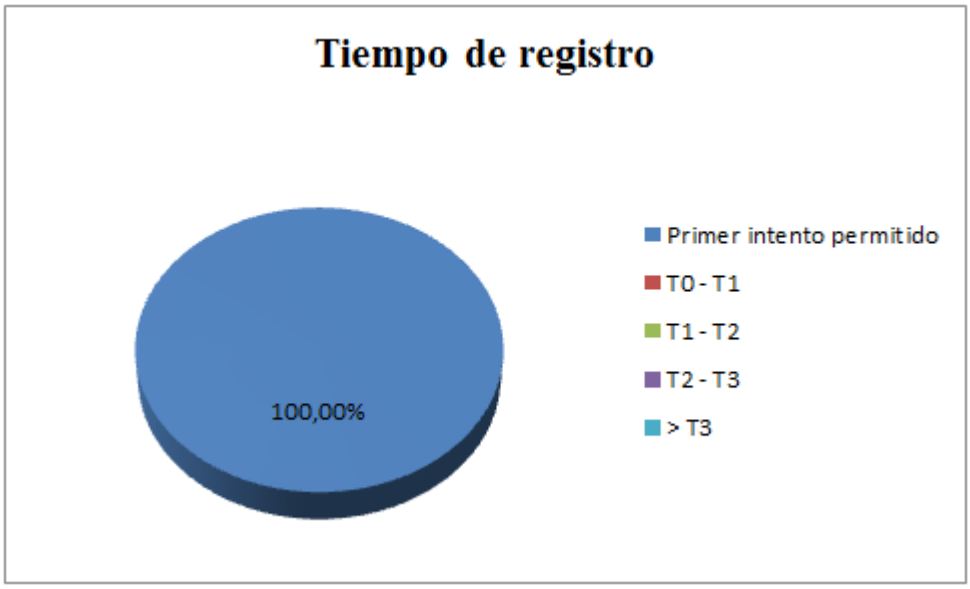

Figura 47: Tiempo de registro escenario 3 previo a la redirección

Todos los casos representan el escenario ideal para el usuario, pues en el primer intento de registro consiguen registrarse en la red para poder disfrutar de los servicios ofrecidos. Sin embargo, como hemos comentando, las redes que poseen un mayor número de usuarios registrados, son aquellas con mejor infraestructura y mejor cobertura a lo largo del país, lo que significará que las tarifas entre las operadoras serán superiores en comparación con el resto de operadoras del país visitado.

La implantación del sistema de redirección tendrá como objetivo forzar el registro de los usuarios en aquellas redes que supongan menos costes y aporten mayores beneficios, pero siempre hay que buscar un equilibrio entre los requisitos comerciales y la calidad de servicio que se le ofrece al usuario final.

6.4 Análisis de requisitos e implantación del sistema redirector

El sistema redirector de tráfico está formado por múltiples servidores agrupados en parejas para ofrecer alta disponibilidad de los diversos servicios que ofrece la plataforma.

Los módulos que componen dicha plataforma son:

- Interfaz Diameter para la comunicación con el HUB de roaming e intercambio de los mensajes de señalización.

- Procesos y aplicaciones que aplican la lógica de la redirección del tráfico.

- Bases de datos.

- Interfaz gráfica de usuario (GUI) para la configuración de las preferencias de las redes y provisión de datos de usuario.

- Módulo de provisión para el procesamiento de las configuraciones y datos de usuario.

- Módulo de envío de alarmas que centraliza el envío de alarmas a los sistemas de monitorización del HUB de roaming.

- Módulo de generación de estadísticas para obtener informes del servicio.

- Interfaz para servidores OTA para el envío de solicitudes de actualización OTA a plataformas externas.

Entre los requisitos comerciales que debe cumplir el sistema redirector cabe destacar que debe tratarse de una implementación multioperadora y que cumpla las recomendaciones recogidas en la especificación sobre redirección de tráfico de la GSMA. La disponibilidad del servicio no será inferior al 99,9% y poseerá mecanismos para la activación y desactivación de la configuración en base al IMSI, al perfil del usuario, país o región, además de mecanismos para detectar las técnicas de *"anti-steering"*, generación de informes y capacidad para poder interactuar con una plataforma OTA externa para poder proporcionar servicios de redirección híbridos.

Los requisitos técnicos cubren aspectos como que debe ser una plataforma activa que capture todos los intentos de registro de los usuarios. Todos los componentes que lo forman se desplegarán en parejas para estar redundantes y evitar así tener un único punto de fallo. Debe ser capaz también de detectar que el sistema no está funcionando correctamente para poder evitar aplicar la redirección al tráfico y provocar una pérdida de servicio a los usuarios. La capacidad y escalabilidad de la solución con básicas para futuras ampliaciones.

Una vez conocidos los requisitos comerciales y técnicos que deben cumplir los sistemas de redirección de tráfico y tener una visión a alto nivel de los componentes que forman la plataforma, describiremos ahora brevemente el proceso de instalación y aceptación del sistema:

1) Elección del emplazamiento: la ubicación geográfica del sistema redirector de tráfico se decidirá en función del espacio disponible en los centros conmutación. El uso de éstos, facilita el despliegue de infraestructura por la infraestructura de comunicaciones IP y transmisión ya desplegadas y acometidas eléctricas ya existentes. Una vez elegido el centro, deberemos buscar ubicación física en la sala de equipos con espacio suficiente para dar cabida a los servidores que forman la plataforma.

2) Diseño de redes IP y de transmisión: en la parte de más compleja del proceso. Basándonos en los requerimientos de conectividad del equipo (puertos físicos, ancho de banda y conectividad con otros sistemas y equipos) diseñaremos una solución para integrarlo con redes existentes. Aspectos como el encaminamiento de red, redundancia de conexiones o apertura de reglas de cortafuegos serán incluidos en el diseño.

3) Instalación física de la plataforma: colocación de los distintos servidores que conforman el sistema redirector en la sala de equipos elegida.

4) Conexión a la acometida eléctrica: además de la redundancia que presentan los servidores a nivel de fuentes de alimentación, las acometidas eléctricas contarán con una fuente alternativa de suministro eléctrico (baterías o grupos electrógenos).

5) Conexión a la red IP.

6) Instalación de las aplicaciones: el proveedor del sistema redirector instalará las aplicaciones y programas encargados de aplicar la lógica de la redirección.

7) Pruebas funcionales: se realizará un conjunto de pruebas de servicio siguiendo las recomendaciones del proveedor de la plataforma con otras pruebas sugeridas por el equipo de diseño de la solución. El objetivo de éstas es certificar el correcto funcionamiento de la plataforma.

8) Pruebas no funcionales: contienen pruebas de carga y rendimiento, generación de alarmas, parada y arranque de servidores, restauración de copias de seguridad entre otras.

La etapa de pruebas funcionales es una de las fases más importantes del despliegue de la plataforma pues se comprobará si el sistema de redirección funciona correctamente. Las pruebas serán realizadas primeramente en un entorno de laboratorio con tráfico simulado por parte de un simulador. Una vez finalicen éstas, pasaremos a un entorno con tráfico real controlado, para comparar los resultados que obtengamos ahora en el entorno de producción con los resultados obtenidos en el laboratorio.

En las siguientes subsecciones se describirán las pruebas funcionales en ambos entornos.

6.4.1 Pruebas funcionales en entorno de laboratorio

El sistema redirector se conectará a un DEA de laboratorio que posee el HUB de roaming y a un simulador de tráfico, tal y como se puede observar en la figura 48.

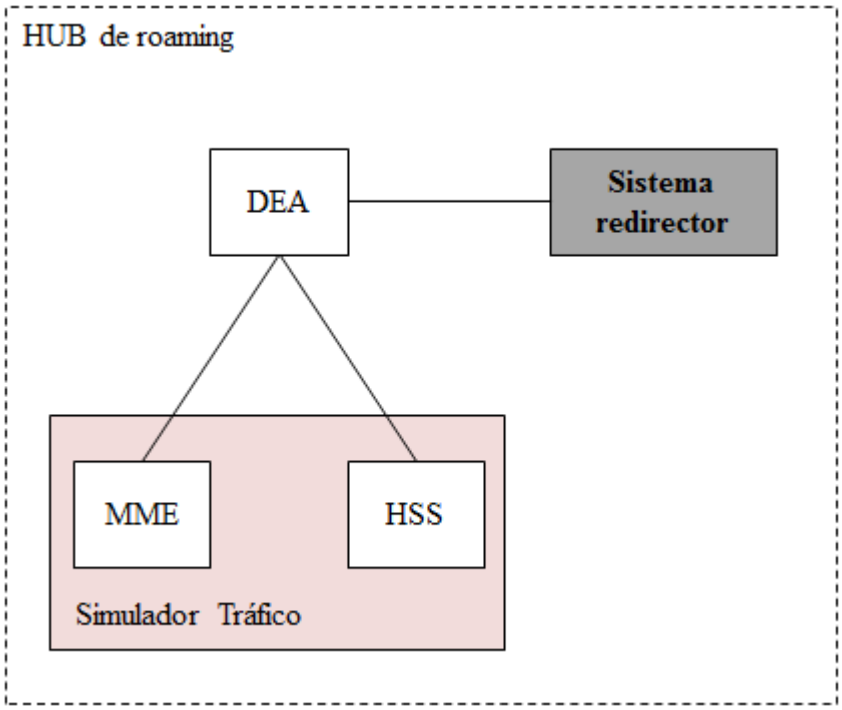

Figura 48: Arquitectura de red del entorno de laboratorio

No se trata de una reproducción exacta del escenario que tendremos cuando el sistema redirector comience a realizar la redirección del tráfico real de la operadora, ya que el objetivo es cerciorar el correcto funcionamiento de la plataforma.

Las pruebas cubren aspectos funcionales, operacionales, de disponibilidad, balanceo de carga de tráfico y rendimiento. Nosotros nos centraremos en las pruebas funcionales realizadas ya que el objetivo de este proyecto fin de carrera es entender cómo se realiza la redirección del tráfico en itinerancia internacional.

Como vimos en el capítulo anterior, la plataforma utiliza códigos de error Diameter para realizar el rechazo del tráfico simulando ser el HSS de la operadora de la que procede el usuario, es decir, la operadora local. La elección del código de error es un aspecto muy importante de la implementación, pues hará variar el comportamiento del terminal móvil, la cantidad de señalización generada entre ambas redes móviles y la efectividad del rechazo.

Se definieron dos códigos de error Diameter en base a la red visitada en la que el usuario está intentando registrarse:

- Red prohibida: se utilizará un código de error no reintentable ya que no queremos en ningún momento el registro de los usuarios en esta red.

- Red no preferida: se utilizará un código de error reintentable, por si el usuario una vez rechazado de la red no encontrara ninguna otra disponible, el registro en ella fuera posible.

A pesar de las recomendaciones de la GSMA recogidas en el IR.73 sobre los códigos de error, se decidió utilizar los dos siguientes en el entorno de laboratorio:

- DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION (5420)

Al tratarse de un error no reintentable, se utilizó como código de error de rechazo para las redes prohibidas. Como vimos en la tabla 5 del capítulo 5, este error puede ser mapeado en el interfaz radio como el error #15 “No suitable cells in tracking area” lo que provoca que el terminal tras el primer rechazo no intente registrarse de nuevo en la red salvo que cambie de área de localización en la red LTE o haya un reintento automático por parte del dispositivo móvil, pero dependerá de la implementación que haya realizado el suministrador del terminal.

En la siguiente traza, podemos observar como el intento de registro es rechazado y el terminal no intenta hacerlo de nuevo, tan sólo observamos mensajes de Device-Watchdog (DWR/DWA):

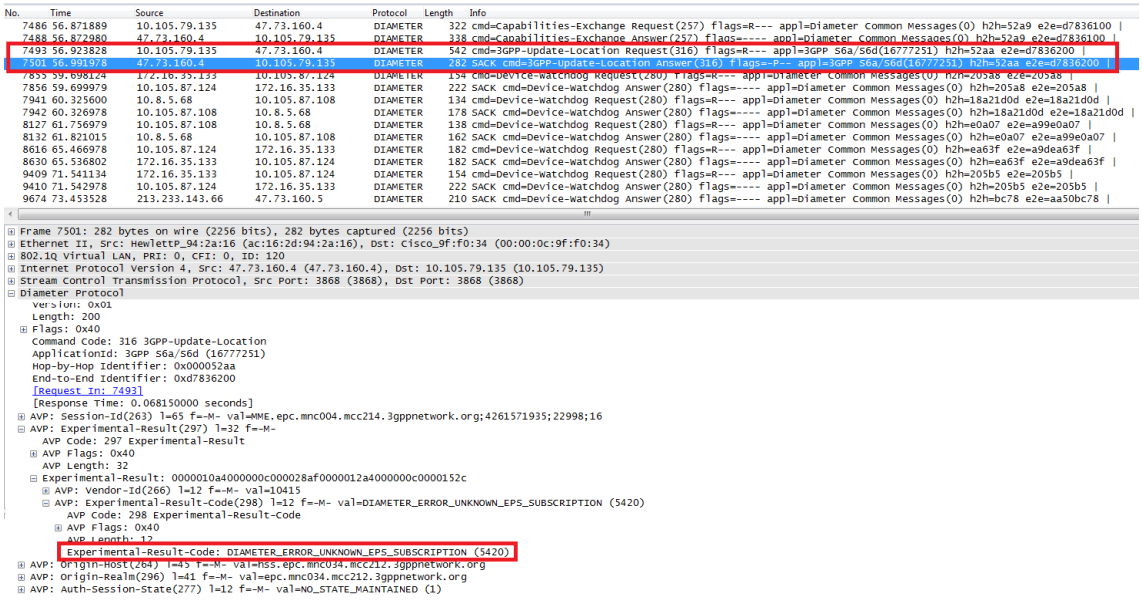

Figura 49: Traza entorno de laboratorio código de resultado 5420

- DIAMETER_INVALID_AVP_VALUE (5004)

Este error es reintentable, es decir, que a pesar de que el usuario es rechazado de la red, más tarde podrá volver a intentar registrarse en ella. Coincide con el comportamiento que esperamos para las redes no preferidas, ya que si la red preferida no está disponible, nuestro deseo será que se conecte a esta.

Tras el primer intento de registro en la red rechazado por el sistema redirector, le seguirán otros cuatro intentos, que serán igualmente rechazados por la plataforma para redirigir al usuario a otra red.

En el caso de que el usuario lanzase un sexto intento de registro, pues no existiese ninguna otra red disponible tras iniciar el procedimiento de selección de nueva red, la plataforma detectará que el terminal está intentando conectarse a la red de forma manual, y en este caso, no será rechazado sino que será aceptado el registro en la red.

En la figura podemos observar como los cinco primeros intentos de registro por parte del terminal son rechazados por la plataforma de redirección.

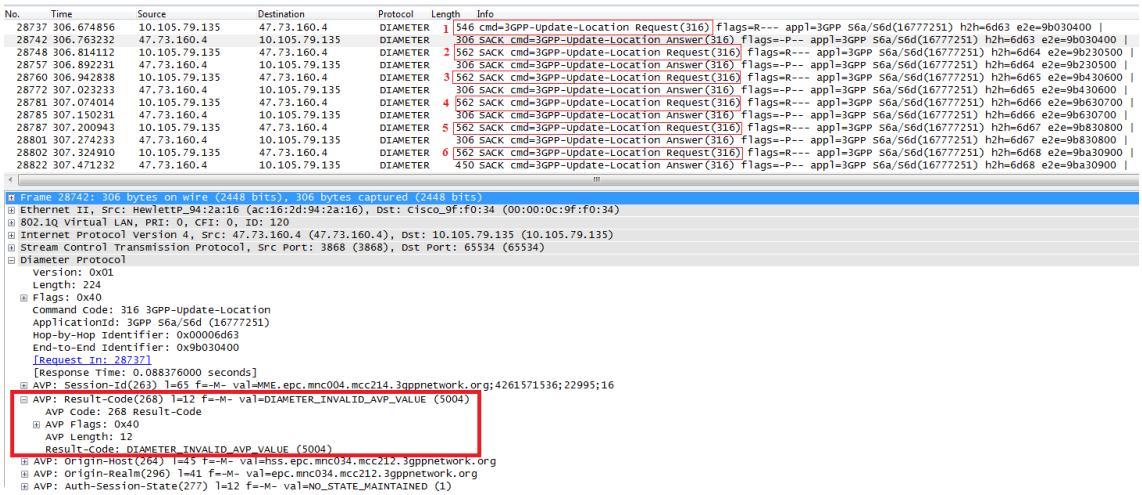

Figura 50: Traza entorno de laboratorio código de resultado 5004

Y el sexto intento de registro es aceptado por la plataforma de redirección.

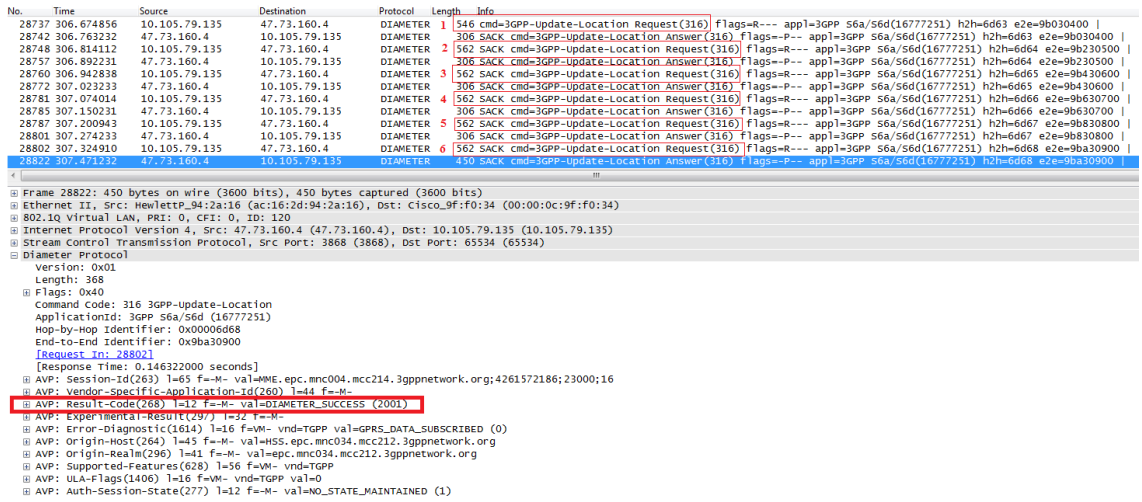

Figura 51: Traza entorno de laboratorio código de resultado 5004, sexto intento de registro

Una vez todas las pruebas funcionales han finalizado, el mismo conjunto de pruebas será realizado en un entorno de producción controlado. El entorno de laboratorio, es un entorno ficticio ya que por ejemplo no podemos simular el interfaz radio, así que los resultados que hemos obtenidos serán provisionales hasta que se realicen los pruebas en el entorno de producción.

6.4.2 Pruebas funcionales en entorno de producción controlado

La realización de pruebas en el entorno de producción, es decir, con tráfico de itinerancia internacional real, no es una tarea sencilla pues la elección de los escenarios y la configuración de las entidades de red ha de efectuarse de forma muy cuidadosa para evitar crear cualquier problema o incidencia que pudiese acarrear una pérdida de servicio para los usuarios.

Para poder llevar a cabo estas pruebas necesitaremos de la colaboración de varias operadoras con las que la operadora de la red local tiene acuerdos de itinerancia internacional. Tarjetas USIM de prueba serán enviadas a sus departamentos de roaming para poder ejecutar dichas pruebas y comprobar el funcionamiento del redirector de tráfico.

Una vez la plataforma de redirección ha configurado esas operadoras como redes preferidas, no preferidas o prohibidas, según esté estipulado en el conjunto de pruebas, puede dar comienzo la nueva fase de pruebas.

Para algunas de las redes que fueron configuradas como redes no preferidas, pudimos observar un comportamiento que no era el esperado y que difería de lo estudiado en el entorno de laboratorio. Para las redes no preferidas se configuró un código de error reintentable para que el usuario pudiera conectarse tras haber sido rechazado de la red por si no hubiese más redes disponibles dentro de la misma tecnología de acceso.

En la plataforma de redirección tan sólo recibíamos un intento de registro LTE y tras ser rechazado, el terminal móvil hacía cinco intentos de registro en la red 2G/3G, es decir, el terminal móvil tras el rechazo en la red LTE hacía un cambio al dominio de circuitos (CSFB, Circuit Switched Fallback).

La siguiente figura muestra el log obtenido del sistema redirector.

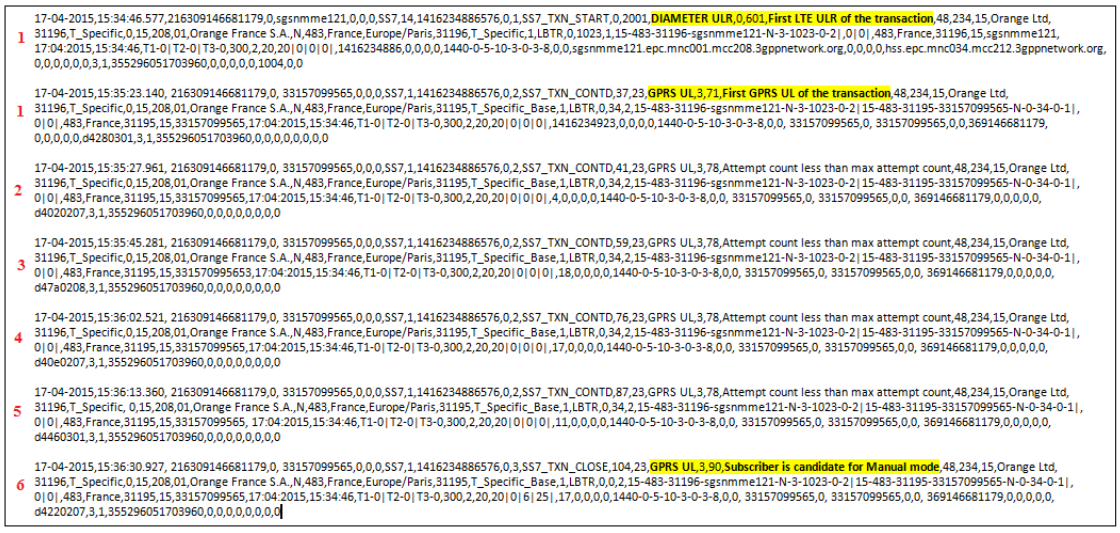

Figura 52: Log del sistema de redirección

Lo primero que podemos observar es el intento de registro en la red LTE y tras ser rechazado, le siguen cinco intentos de registros en el dominio de circuitos, concretamente, que son rechazados también. Al existir un nuevo intento de registro en el dominio de circuitos, el sistema redirector asume que el terminal móvil está intentando conectarse a la red de forma manual, así que este sexto intento será aceptado por la plataforma.

En la siguiente figura se describirá el flujo de mensajes que ha existido en la red para una mejor comprensión del escenario que estamos estudiando.

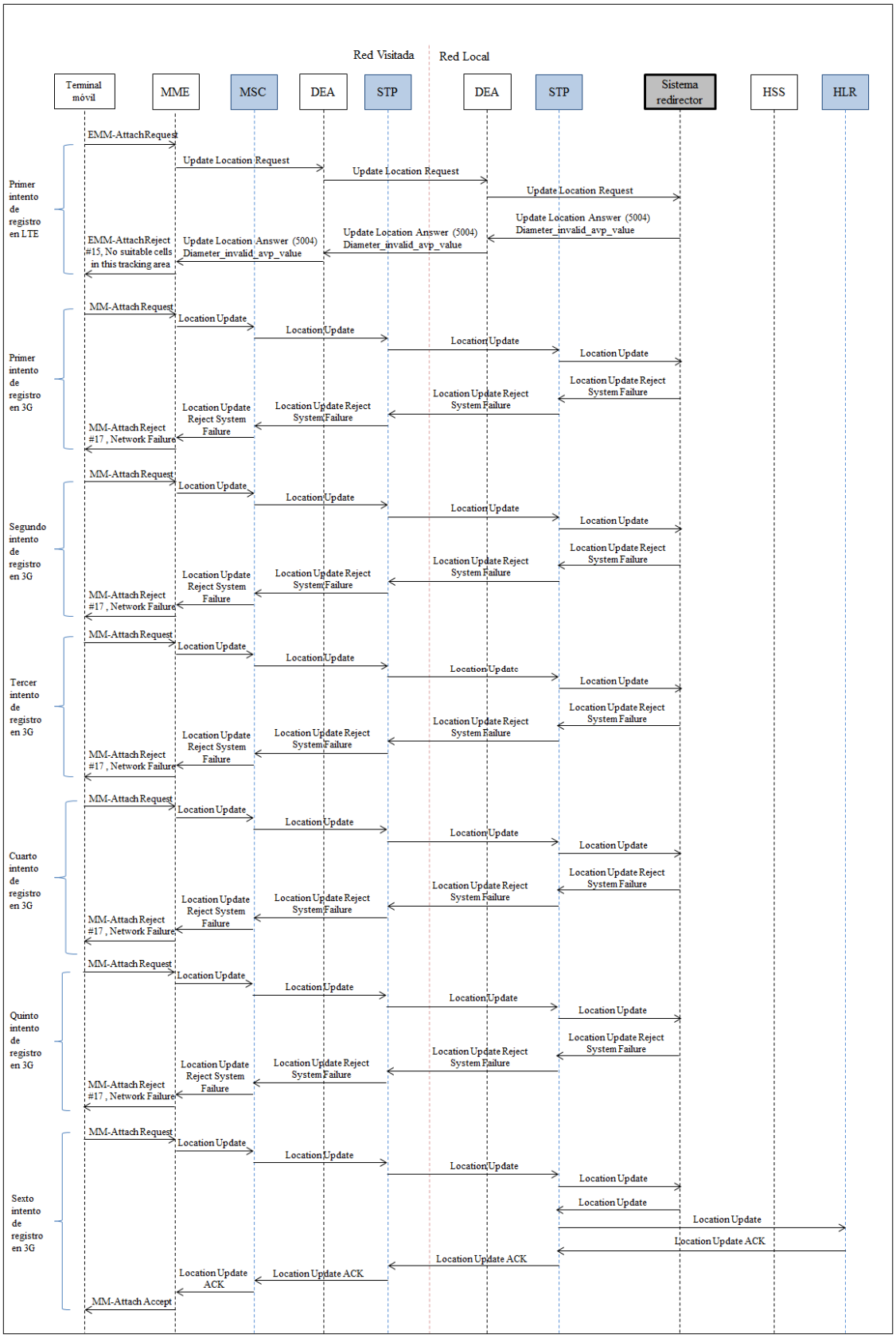

Figura 53: Diagrama de mensajes de las pruebas realizadas en el entorno de producción

El comportamiento anómalo del terminal era debido a un mapeo incorrecto del código de error Diameter 5004 (DIAMETER_ERROR_INVALID_AVP) en el código del interfaz radio que es propagado hasta el dispositivo móvil. Éste mapeo es realizado por el MME de la operadora de la red visitada que en lugar de enviar el código de error radio #17 “Network Failure” estaba enviando el código #15 “No suitable cells in tracking area”.

Tras el estudio de los resultados de las pruebas realizadas en diferentes redes, detectamos que era una situación bastante habitual que el error Diameter 5004 (DIAMETER_ERROR_INVALID_AVP) no estuviese correctamente mapeado en el interfaz radio, provocando de esa manera, una experiencia de usuario no óptima al cliente de la operadora local.

Se decidió entonces cambiar los códigos de rechazo y la lógica configurada en la plataforma de redirección. En lugar de utilizar dos códigos diferentes de rechazo en base a si la red es no preferida o prohibida, se comenzaría a utilizar un único código de rechazo para ambos tipos de red.

El código elegido es uno de los códigos recomendados por la GSMA, DIAMETER_UNABLE_TO_COMPLY (5012). Se trata de un error reintentable, así que es perfecto para las redes no preferidas, pero, ¿qué ocurre con las redes prohibidas? Si la red a la que se quiere aplicar redirección de tráfico de trata de una red prohibida, la plataforma de redirección estará configurada para rechazar todos los intentos de registro que pueda realizar.

No se trata de la causa más efectiva o beneficiosa tanto para la operadora como para el usuario, ya que la señalización entre ambas operadoras aumentará pudiendo provocar problemas de congestión en alguna de ellas. El usuario además tardará más tiempo en obtener servicio por parte de la red, pues tras cinco intentos de registro rechazados, iniciará el proceso de selección de red para poder registrarse en ella. La ventaja que tenemos utilizando este código de error, es que el mapeo del código de error en el interfaz radio se realiza correctamente en todas las operadoras siguiendo las recomendaciones de las especificaciones.

6.5 Migración de tráfico al sistema redirector y activación de la redirección

El procedimiento para migrar el tráfico de itinerancia internacional de la operadora al sistema redirector es muy parecido al descrito en la sección 6.2 de este mismo capítulo, pero en este caso, no tendremos que migrar todo el tráfico, sino sólo los mensajes relacionados con el registro del usuario en red, es decir, los mensajes Diameter “Update Location Request”.

Cuando los DEAs del HUB de roaming reciben todo el tráfico de itinerancia internacional de la operadora, serán capaces de diferenciar los distintos tipos de mensaje en función del código de comando Diameter. Para los mensajes “Update Location Request” el código de

comando es 316, así que los DEAs filtrarán el tráfico en base a este código para encaminar sólo estos mensajes a la plataforma de redirección.

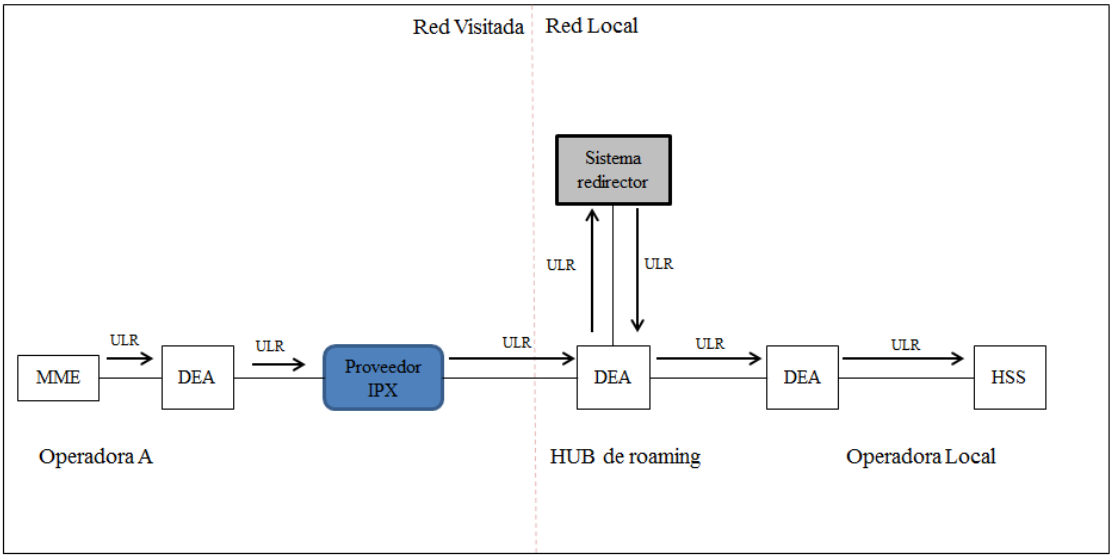

Figura 54: Arquitectura del HUB de roaming sin la activación de la redirección del tráfico

Una vez todos los mensajes de "Location Update Request" están migrados a la plataforma, debemos configurar el sistema redirector con la distribución de preferencias que desea la operadora para cada red de los países con los que tiene acuerdo de itinerancia internacional. Para ello, nos entregará una lista identificando a cada una de las operadoras por el nombre, el código TADIG (Transferred Account Data Interchange Group), el IMSI y si debe ser red preferida, no preferida o prohibida para poder configurar la plataforma de forma adecuada pero sin todavía aplicar la redirección al tráfico.

Código TADIG	País	Nombre Operadora	IMSI	realm	Configuración Plataforma
POLKM	Polonia	Polkomtel	26001	epc.mnc001.mcc260.3gppnetwork.org	No preferida
POL02	Polonia	T-Mobile	26002	epc.mnc002.mcc260.3gppnetwork.org	Prohibida
POL03	Polonia	Orange	26003	epc.mnc003.mcc260.3gppnetwork.org	Preferida
CANRW	Canadá	Rogers	302720	epc.mnc720.mcc3023gppnetwork.org	Preferida
CANTS	Canadá	Telus	302220	epc.mnc220.mcc3023gppnetwork.org	No preferida
CANMC	Canadá	Fido	302370	epc.mnc370.mcc3023gppnetwork.org	Prohibida

Tabla 8: Documento configuración preferencias operadoras del sistema redirector

Una vez la plataforma de redirección está configurada y los mensajes de localización Diameter han sido migrados, podemos dar paso a la última fase del proceso, que es la activación de la redirección del tráfico.

No se hará en una única etapa para asegurar el correcto comportamiento de la plataforma y evitar cualquier problema en el tráfico que se está redireccionando.

Se elegirán un par de países en los que se activará la redirección del tráfico primero y se mantendrán en observación durante una semana. A través de las herramientas de monitorización disponibles, se revisará si el tráfico está siendo redirigido correctamente, comprobando si los usuarios se registran a las redes según los valores esperados y si el código de rechazo es el configurado en la plataforma.

A continuación, se activará la redirección para el resto de países y se llevarán a cabo las mismas tareas de monitorización revisando cada una de las relaciones de itinerancia internacional que están siendo encaminadas a través de la plataforma. Pasada una semana de la activación, sacaremos un informe de la distribución de los usuarios en los diferentes países para comenzar a ver los efectos de la redirección en el tráfico.

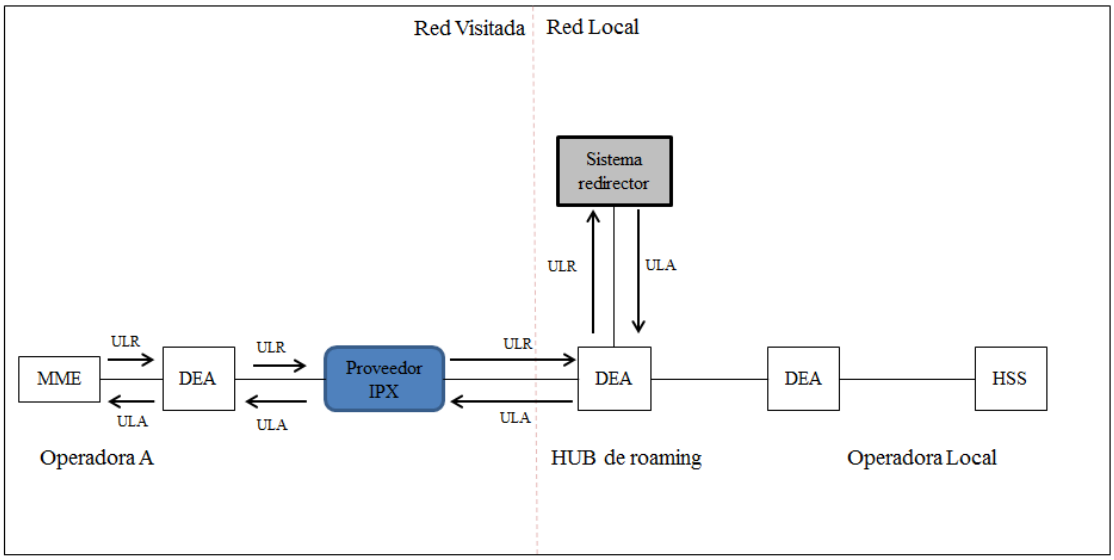

Figura 55: Activación de la redirección del tráfico por parte de la plataforma

6.6 Análisis de los escenarios tras la redirección del tráfico

Ahora que la redirección ha sido activada, podemos realizar un análisis comparativo de los tres escenarios bajo estudio para comprobar la efectividad en la redirección de los usuarios hacia las redes que nosotros deseemos.

Escenario 1: país visitado con tres redes móviles denominadas operadora A, operadora B y operadora C.

Dada la configuración de cada una de las operadoras en el sistema redirector, es decir, la operadora A como red preferida, la operadora B como no preferida y la operadora C como la red prohibida, esperamos que tras la redirección del tráfico, la mayor parte de los

usuarios sean redirigidos hacia la red preferida. En la siguiente gráfica podemos observar la distribución de usuarios que hemos obtenido ahora.

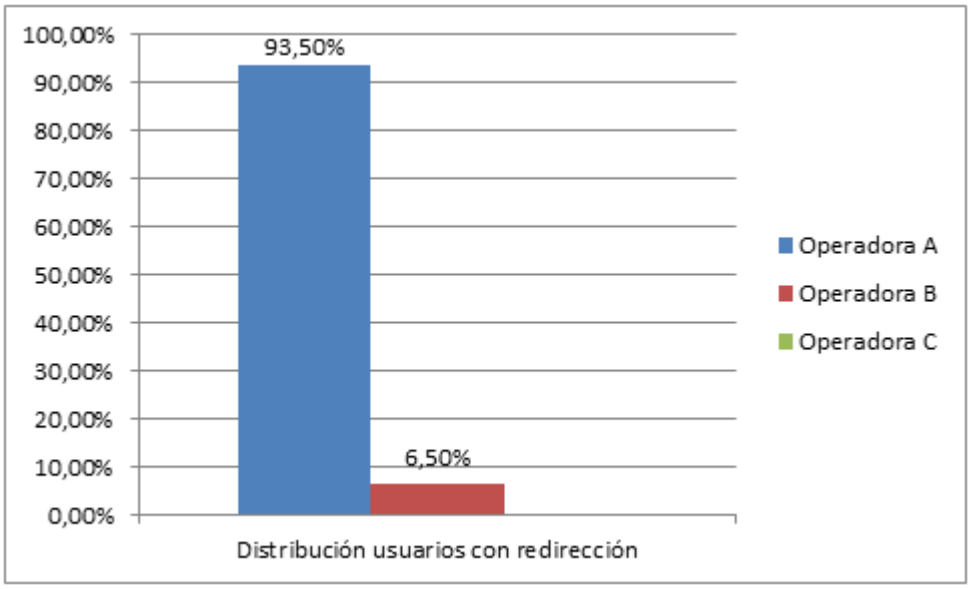

Figura 56: Distribución usuario en escenario 1 tras la redirección

Claramente, la redirección ha sido muy eficaz pues más del 93% de los usuarios se han registrado en la red preferida, es decir, en la operadora A y ningún usuario ha sido capaz de registrarse en la red configurada como prohibida, que sería la red de la operadora C. A pesar de que el código de rechazo de nuestro sistema redirector es un código reintentable, la plataforma rechazará todos los intentos de registro en la red prohibida, es decir, una vez llegado al número máximo de reintentos en LTE, que es cinco, si el terminal móvil sigue intentando registrarse en la red prohibida, nuestra plataforma continuará rechazando los intentos de registro.

Tan sólo un 6,5% de los usuarios se han registrado en la red no preferida, la operadora B, seguramente porque se encontraban en una zona geográfica en la que la operadora A no tenía buena cobertura móvil o estaban realizando el registro en la red de forma manual. Tras cinco rechazos consecutivos por parte de la plataforma de redirección, el sexto intento sería aceptado para permitir el registro en la red no preferida. En la siguiente figura veremos de forma muy clara la redistribución de los usuarios entras las redes disponibles tras la aplicación de la redirección.

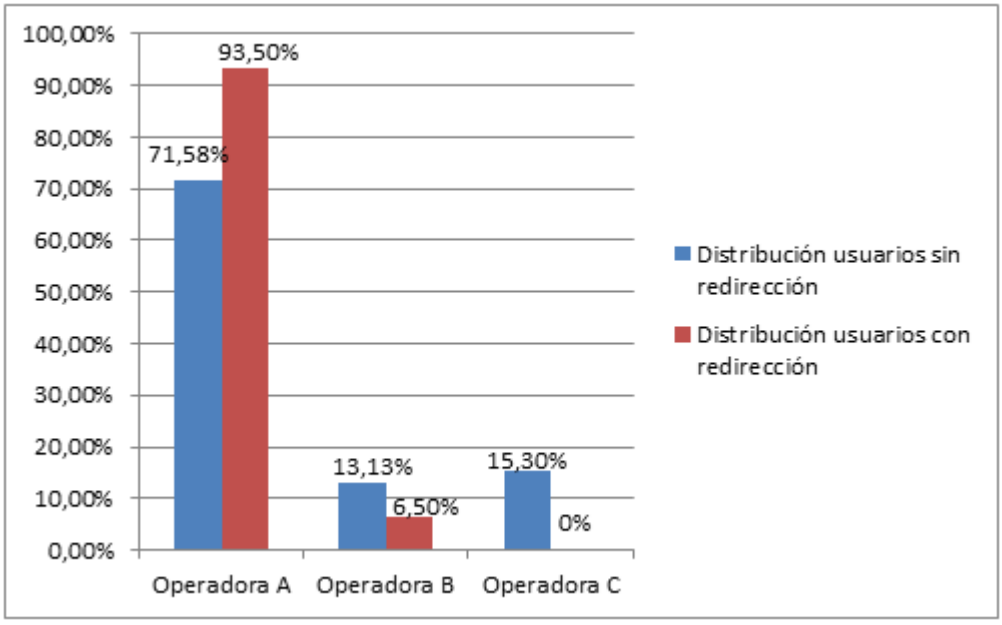

Figura 57: Comparativa distribución de usuarios en escenario 1

El porcentaje de usuarios que previa a la redirección del tráfico se registraba en la red de la operadora C, ha sido sumado a la red de la operadora A. Vemos también que el porcentaje de usuarios registrados en la red de la operadora B ha disminuido, lo que significa que hay zonas geográficas del país donde las redes de las operadoras A y B tienen cobertura, pero tras la aplicación de la redirección, los usuarios que tan sólo que han intentado registrarse de forma manual o que la cobertura de la red de la operadora A no era suficiente han conseguido registrarse en la red de la operadora B.

Al entrar en juego los reintentos de registro en la red, el tiempo que tardan los usuarios en acceder a los servicios no será el mismo que el obtenido cuando no existía la redirección del tráfico en la red. La siguiente figura muestra los tiempos de registro según los umbrales definidos para calificar la calidad de servicio que es percibida por el usuario.

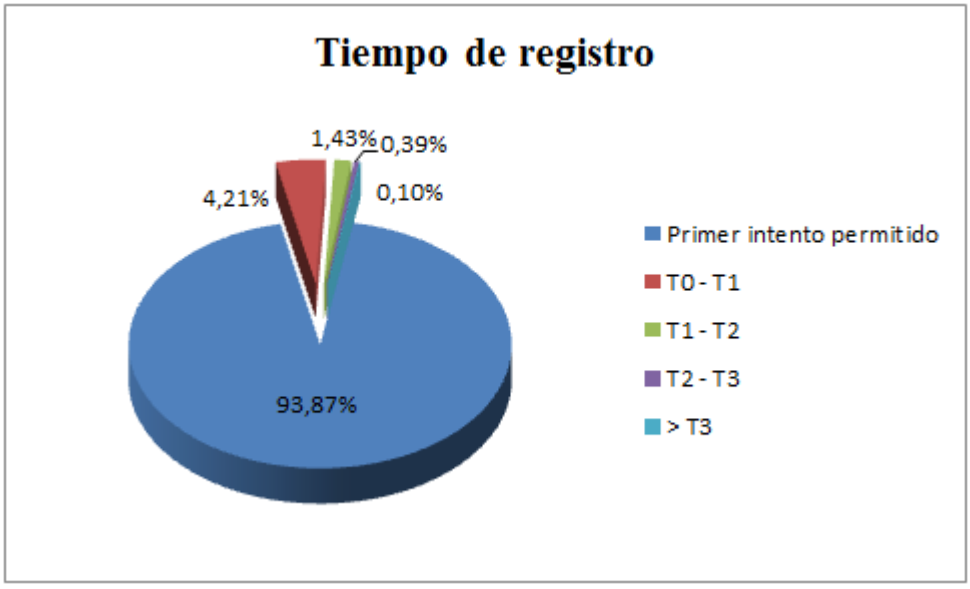

Figura 58: Tiempo de registro escenario 1 tras la redirección

En la tabla, además del porcentaje de usuarios registrados en función del umbral de tiempo definido previamente, se encuentra el valor medio del tiempo que tardan los usuarios en registrarse para cada umbral.

Umbral de tiempo	% Registros de usuario	Tiempo medio de registro (segundos)
T0	93,87%	0
T0 - T1	4,21%	72,17
T1 - T2	1,43%	152,83
T2 - T3	0,39%	170,09
> T3	0,10%	2482,54

Tabla 9: % de registros por umbral y tiempo medio de registro en escenario 1

Más del 93% de nuestros usuarios se han registrado bajo el umbral T0, es decir, no han necesitado ser redirigidos hacia la red preferida y en el primero intento han conseguido registrarse. La calidad de servicio que perciben es inmejorable pues desde el primer momento se encuentran registrados en la red.

Los usuarios que se encuentran en el umbral T0 – T1 son aquellos que intentaron registrarse en la red no preferida o red prohibida y tras cinco rechazos, fueron redirigidos a la red preferida. Los reintentos se realizan cada 10 segundos y el número máximo de reintentos antes de realizar una nueva selección de red es 5, dando como resultado el tiempo medio de registro para este umbral.

Los usuarios que se encuentran en el umbral T1 – T2 intentaron registrarse primero en la red no preferida y en la red prohibida (o viceversa) antes de ser redirigidos hacia la red preferida.

En el umbral T2 – T3 y > T3 encontramos usuarios que han intentado registrarse en la red prohibida y en la red no preferida varias veces antes de ser redirigidos hacia la red preferida. Seguramente se hayan intentado registrar de forma manual en la red prohibida, y la plataforma haya rechazado cada uno de los intentos de registro, hasta que el usuario ha decidido cambiar su selección manual hacia otra red para obtener servicio.

A pesar de ser un porcentaje muy pequeño los usuarios que han conseguido registrarse en el último umbral, es decir, a partir de 180 segundos, podemos observar que el tiempo medio de registro es de casi 2.500 segundos. A pesar de tener configurado el valor T3 como el valor máximo que aplicaremos redirección a los usuarios, debemos recordar que si el intento de registro procede de una prohibida, el temporizador no aplica y el sistema redirector continuará rechazando el tráfico.

Escenario 2: país visitado con tres redes móviles denominadas operadora D, operadora E y operadora F.

En este segundo escenario tenemos las operadoras D y F configuradas como redes no preferidas y la operadora E como red preferida. La mayor parte de los usuarios se registrarán en la red preferida, ya sea porque el usuario intenta conectarse en primera

instancia en ella o porque ha sido redirigido. Habrá un porcentaje pequeño de usuarios que se repartirá en las operadoras configuradas como no preferidas.

Casi el 90% de los usuarios se registran en la red preferida, es decir en la operadora E, mientras que el 10% restante se redistribuye entre las redes no preferidas.

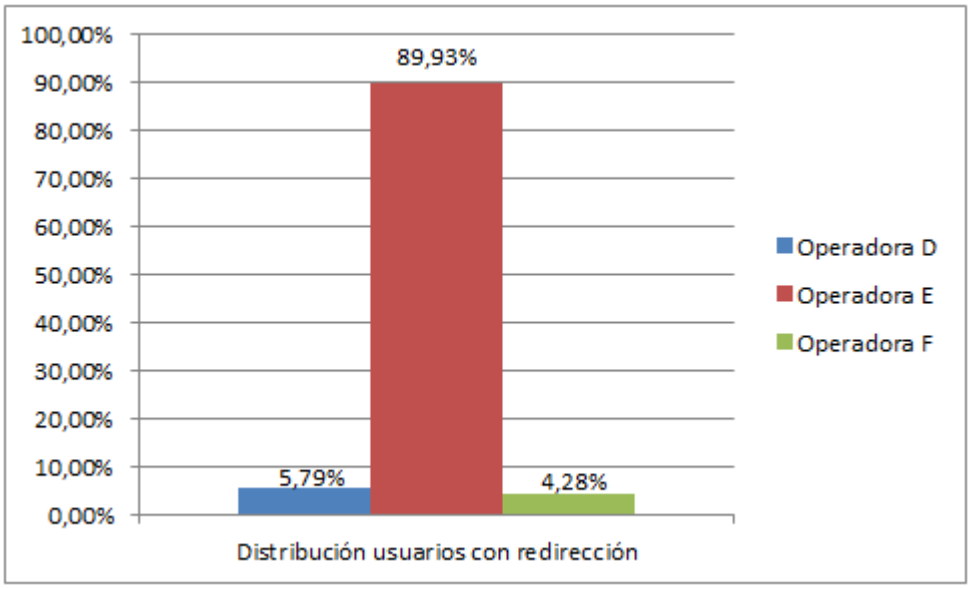

Figura 59: Distribución de usuarios en escenario 2 tras la redirección

Comparando los resultados obtenidos antes y después de la redirección de tráfico, podemos observar como la red preferida acoge a casi todos los usuarios que están intentando registrarse. En el escenario previo a la redirección, la distribución de usuarios era completamente diferente.

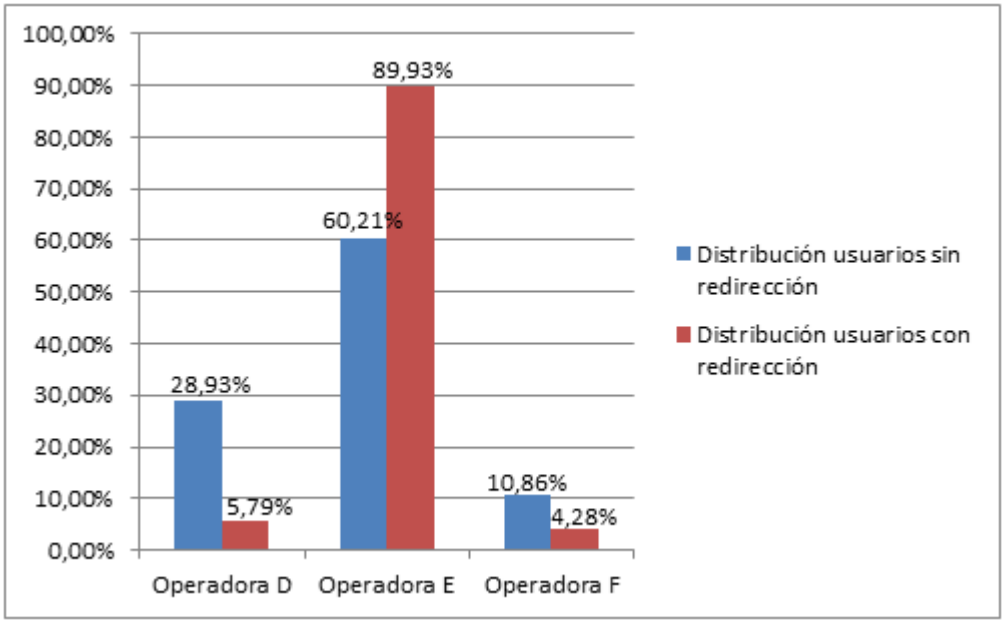

Figura 60: Comparativa distribución de usuarios escenario 2

Basándonos en términos de redirección, la configuración del sistema redirector del escenario 1, es decir, una red preferida, una red no preferida y otra prohibida, es mucho más efectiva que la configuración realizada para las redes del escenario 2, ya que se consigue la mayor distribución de usuarios registrados en una de las redes. La elección de red preferida, no preferida o prohibida, aparte de basarse en cobertura móvil que pueda tener en el país la operadora y la infraestructura de buena calidad desplegada, tienen en cuenta los intereses comerciales. Las tarifas entre operadoras no son iguales para todas las relaciones de itinerancia internacional, sino que deben ser negociadas entre las entidades comerciales de cada operadora. Si se consiguen unas tarifas más baratas en cierta operadora, se configurará el sistema redirector para redirigir el mayor número de usuarios a esa operadora o al menos el número de usuarios acordados.

El porcentaje de usuarios que han perdido las redes de las operadoras D y F, es debido a la redirección de usuarios que se produce hacia la red preferida, pero aun así mantiene, casi un 11% de los usuarios totales seguramente porque la cobertura de la red preferida no es total en el país, algo que entra dentro de la normalidad.

Estudiemos ahora el tiempo que tardan los usuarios en registrarse en la red. Como en el escenario anterior, mostraremos los porcentajes de usuarios registrados según los umbrales de tiempo definidos y en la tabla tendremos el tiempo medio para cada uno de los umbrales.

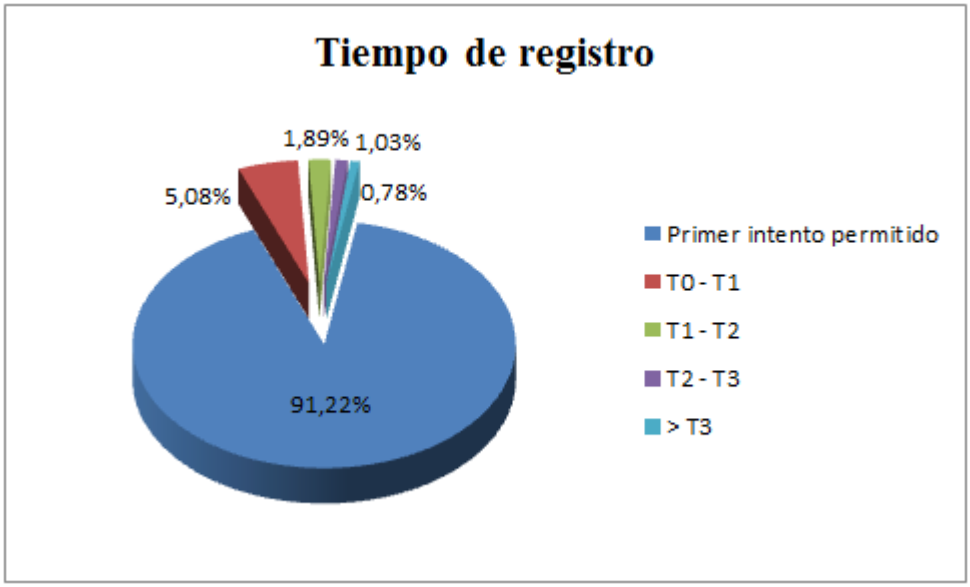

Figura 61: Tiempo de registro escenario 2 tras la redirección

Umbral de tiempo	% Registros de usuario	Tiempo medio de registro (segundos)
T0	91,22%	0
T0 - T1	5,08%	51,03
T1 - T2	1,89%	98,76
T2 - T3	1,03%	161,12
> T3	0,78%	203,43

Tabla 10: % de registro por umbral y tiempo medio de registro en escenario 2

Prácticamente todos los usuarios van a percibir una calidad de servicio excelente o muy buena, ya que más del 91% de ellos se registran en la red preferida en el primer intento y algo más del 5% de los usuarios se registran tras haber sido redirigidos desde las redes configuradas como no preferidas o porque la plataforma de redirección ha detectado registro manual por parte del usuario y tras cinco rechazos, el nuevo intento de registro es aceptado.

Disminuye de forma notable el tiempo medio de registro para todos los umbrales de tiempo y en concreto para el último, ya que al ser redes no preferidas, una vez el temporizador de 180 segundos es alcanzado, los siguientes registros que reciba el sistema de redirección, serán aceptados.

Si comparamos los resultados obtenidos en este escenario con respecto al anterior, vemos una mejora significante en el número de usuarios que consiguen registrarse en la red en un período inferior a 80 segundos, ya que las redes configuradas como no preferidas, si detectan modo manual de registro, es decir, un sexto intento de registro consecutivo, aceptarán el registro del usuario en la red.

Escenario 3: país visitado con tres redes móviles denominadas operadora G, operadora H y operadora I.

En este último escenario, tenemos una red configurada como preferida, que se trata de la operadora I y las otras dos operadoras, están configuradas como red prohibida. Con dicha configuración en el sistema de redirección, esperamos que el 100% de los usuarios se registren en la red preferida, pues los intentos de registro en las redes prohibidas serán rechazados de forma indefinida.

La distribución de usuarios obtenida tras la redirección es mostrada en la siguiente figura.

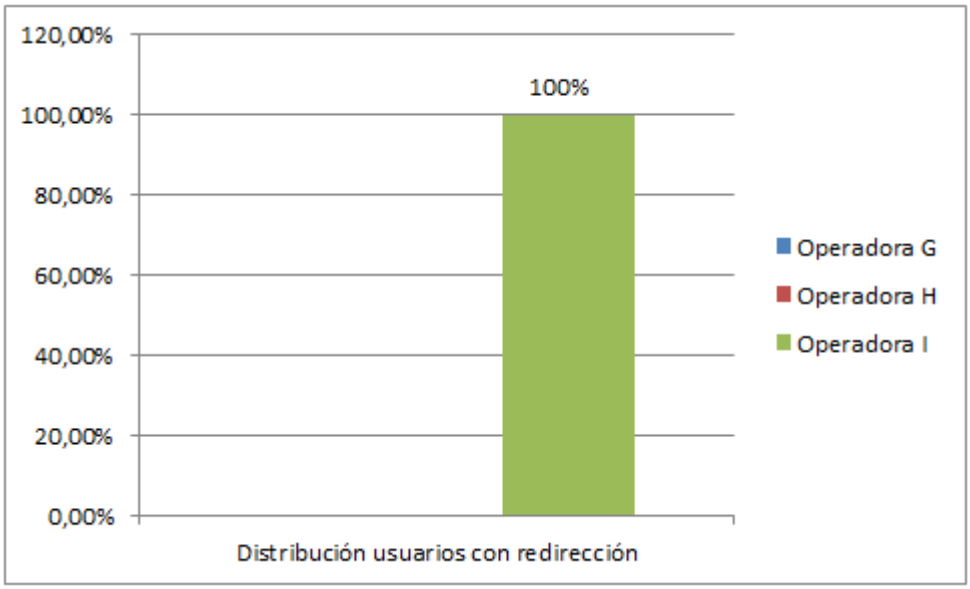

Figura 62: Distribución de usuarios en escenario 3 tras la redirección

Puede parecer el escenario ideal, pues hemos conseguido una efectividad en la redirección del 100%. Sin embargo, en la gráfica sólo se muestran los usuarios que han conseguido registrarse en la red, que en este tipo de escenarios nunca es la totalidad de ellos. Un 9% de los usuarios que intentaban registrarse en la red, se quedaron sin servicio probablemente porque intentaban registrarse en alguna de las redes prohibidas de forma indefinida mediante el procedimiento manual o se encontraban en un área del país donde la red preferida no tenía cobertura. Es una situación nada deseable para las operadoras de la red local, pues parte de sus abonados no pueden acceder a los servicios cuando se encuentran en el extranjero.

La siguiente figura muestra la comparación de la distribución de usuarios antes y después de la redirección, pero no es realista, porque no tiene en cuenta a los usuarios que se han quedado sin acceso al servicio.

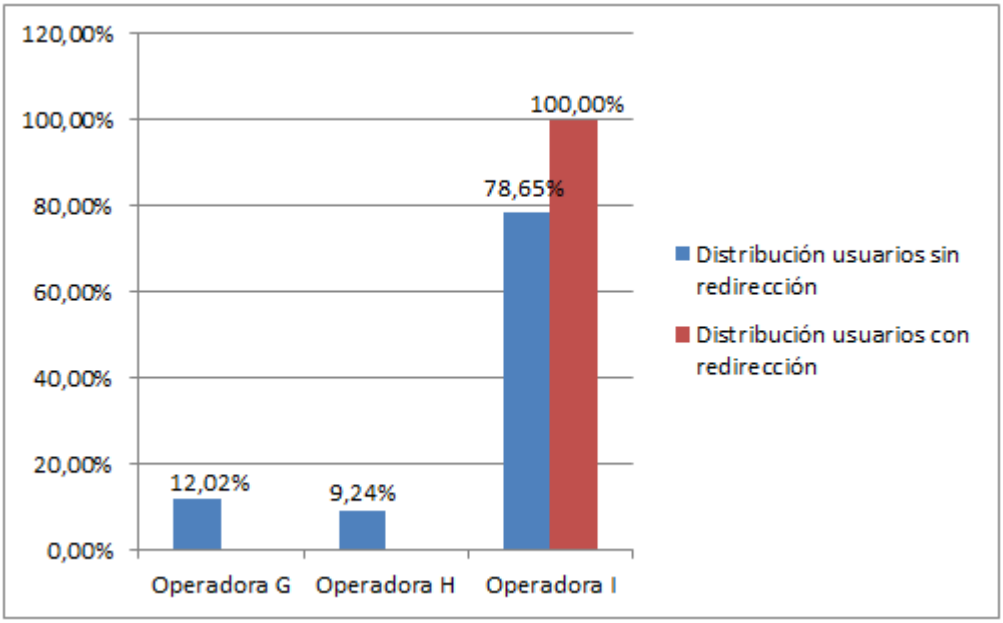

Figura 63: Comparativa distribución de usuarios escenario 3

Podemos imaginar que la configuración del sistema redirector en este escenario, afectará a los tiempos que tardan los usuarios en registrarse en la red.

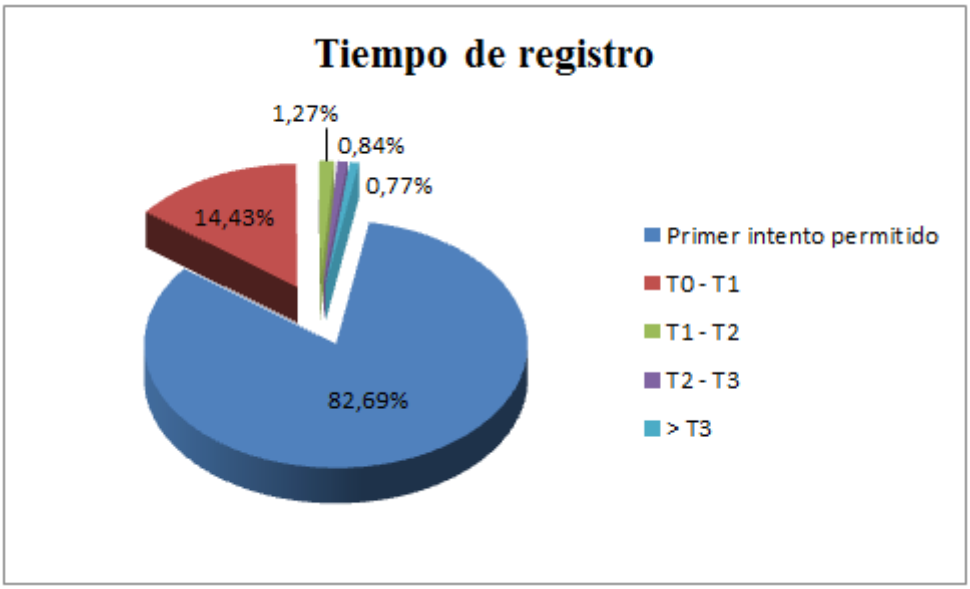

Figura 64: Tiempo de registro en escenario 3 tras la redirección

Al existir una única red en las que los usuarios pueden registrase, el número de éstos que lo consiguen en el primer intento ha disminuido significativamente en comparación con los escenarios anteriores, en este caso de estudio no llega el 83% de los usuarios.

Cabe resaltar también los usuarios que consiguen registrarse en el período comprendido entre T0 y T1, es decir, más de un 14% de los usuarios tras intentar el registro en cada una de las redes prohibidas, es redirigido hacia la red preferida.

Umbral de tiempo	% Registros de usuario	Tiempo medio de registro (segundos)
T0	82,69%	0
T0 - T1	14,43%	78,63
T1 - T2	1,27%	122,56
T2 - T3	0,84%	173,09
> T3	0,77%	2688,43

Tabla 11: % de registro por umbral y tiempo medio de registro en escenario 3

El tiempo que tardan un porcentaje pequeño de usuarios en registrarse en red se dispara, tardando casi 2.700 segundos en tener acceso a los servicios de la red.

Este tercer escenario es el menos favorable, porque a pesar de haber conseguido la mejor redirección del tráfico hacia la red preferida, un porcentaje de usuarios se queda sin servicio lo que se sumará a las quejas por la pobre calidad de servicio percibida pues tardan más tiempo en acceder al servicio.

Este tipo de escenario basado en una redirección agresiva del tráfico, obtendría mejores resultados en base a la calidad de servicio percibida por el usuario, si se utilizara un código no reintentable para rechazar el tráfico. Tras un rechazo en cada red prohibida el usuario se registraría en la red preferida en un intervalo de tiempo inferior seguramente a 30 segundos.

En base a los resultados obtenidos antes y después de aplicar la redirección del tráfico, hacemos un balance final de los aspectos que influyen en la eficiencia y calidad de servicio percibida por el usuario final:

- La cobertura de la operadora móvil es un factor clave ya que cuando no la hay, los usuarios no pueden ser redirigidos o en caso de serlo, los tiempos promedio de registro se disparan.

- La configuración de la tarjeta USIM condiciona los resultados de la redirección, ya que el sistema no podrá aplicar la redirección de forma correcta. Una configuración apropiada de la tarjeta USIM mejorará el efecto de la redirección.

- Las causas de rechazo no reintentables tan sólo se deberían utilizar cuando se tenga la certeza de una cobertura excelente de la red preferida o se posea algún sistema de redirección dinámica para actualizar la SIM de los usuarios, de lo contrario, los tiempos de registro aumentarán.

- Las causas de rechazo no reintentables son ideales para redes prohibidas ya que no queremos el registro de ningún usuario en ella. El tiempo de registro será menos pues tras un primer rechazo el usuario es redirigido hacia otra red.

- Las causas de rechazo no reintentables son óptimas para las redes no preferidas, ya que se permite el registro del usuario tras 5 rechazo consecutivos al intento de registro.

- La configuración ideal es aquella que tiene una red preferida, una red no preferida y otra red prohibida, ya que se fomenta el registro rápido en la red preferida mediante el bloqueo de una de las redes restantes. Se mantiene una red como no preferida para permitir el registro de los usuarios en aquellas zonas geográficas de mala cobertura de la red preferida,

Capítulo 7

Conclusiones y líneas futuras

7.1 Conclusiones

Uno de los grandes retos a los que se tiene que enfrentar una operadora es buscar el equilibrio entre el coste que supone ofrecer una calidad de servicio aceptable con la captación de los ingresos necesarios para afrontar las inversiones que deben realizarse en la redes y la creación de nuevos servicios.

La situación no es trivial pues la disminución de los precios relativos al tráfico de itinerancia internacional hace que cada año el volumen de ganancias se vea disminuido ya que los costes de mantenimiento de las redes asociados son iguales o mayores. Por ello, la utilización de sistemas redirectores de tráfico, objetivo de este proyecto fin de carrera, ayudan a disminuir los costes del servicio de itinerancia internacional y a ofrecer la mejor calidad de servicio posible al cliente final.

A lo largo del proyecto, hemos ido revisando los conceptos claves que se han convertido en hitos básicos para el gran éxito que ha supuesto la itinerancia internacional dentro de las comunicaciones móviles.

La introducción de los HUBs de roaming ha supuesto toda una revolución, pues facilitó el aumento y la sencillez del número de aperturas de nuevos acuerdos de itinerancia internacional, provocando una gran satisfacción en los abonados pues podían estar haciendo uso de los servicios a los que estaban acostumbrados en cualquier parte del mundo. Se ha desarrollado brevemente cada una de las fases para que todo el tráfico de

itinerancia internacional de una operadora se encontrara centralizado, ya que suponía un requisito básico para poder aplicar redirección.

Las plataformas de redirección del tráfico de itinerancia internacional han supuesto un paso más en el camino emprendido hace muchos años. Estos sistemas han permitido a las operadoras tener el control sobre sus usuarios cuando se encuentran en el extranjero, forzando el registro en aquellas redes que tuviesen una mejor calidad de servicio y fueran redes beneficiosas desde el punto de vista comercial. Normalmente la calidad de servicio y las redes beneficiosas comercialmente son términos opuestos, así que es labor de los equipos comerciales y técnicos llegar a un consenso para decidir a qué redes deben ser redirigidos los usuarios.

Se ha descrito con un alto grado de detalle técnico el funcionamiento de estas plataformas así como los requisitos básicos para su implementación. Gracias a las pruebas realizadas en el entorno de laboratorio y en un entorno controlado de tráfico real, hemos podido desarrollar y poner solución a los problemas que surgen cuando un nuevo servicio es desplegado en las operadoras móviles y existe la interacción con otras operadoras móviles sobre las que no tienes el control.

Las recomendaciones descritas en cada una de las especificaciones consultadas para la realización de este proyecto fin de carrera han sido básicas, que junto con el trabajo diario realizado en este entorno, han dado fruto a una profunda compresión del servicio y a un análisis de los requerimientos para mejorar la calidad del servicio de itinerancia internacional.

7.2 Líneas futuras

La regulación europea aplicada al servicio de itinerancia internacional forma parte de un gran proyecto para reformar el mercado de las telecomunicaciones y hacerlo más competitivo frente a los grandes mercados como son Estados Unidos y los países asiáticos. Las operadoras deberán asumir grandes retos técnicos y comerciales para poder cumplir con las normas impuestas y a su vez, maximizar los ingresos y minimizar los costes.

En el año 2011, la Comisión Europea planteó la posibilidad a los usuarios de firmar un contrato con otra operadora móvil para los servicios de itinerancia internacional con fecha de comienzo el 1 de Julio del 2014 dentro de los países que conforman la Unión Europea. Sería una operadora diferente a la contratada en el país de origen del usuario y no le sería necesario cambiar de dispositivo móvil o tarjeta USIM. El objetivo de esta nueva regulación pretende abaratar el precio del servicio de itinerancia internacional y fomentar la competitividad del sector. Los usuarios podrán así escoger un proveedor de servicios en itinerancia internacional más barato en el que se registrarían de forma automática al viajar al país deseado.

Este sistema facilitará la entrada de **proveedores alternativos de itinerancia internacion**al, denominados en inglés como **ARP (Alternative Roaming Provider**) e incluso a los operadores móviles virtuales (OMV), a los que las operadoras de los estados

miembro de la Unión Europea deberán permitir el acceso a sus redes mediante precios regulados.

Sin embargo, hasta que no se ha hecho oficial el fin a los sobrecostes infligidos a los usuarios por el servicio de itinerancia internacional a partir de Junio del 2017, esta posibilidad no ha sido tomada en consideración por las operadoras móviles.
El reglamento sobre itinerancia aprobado por el conjunto de reguladores europeos de comunicaciones electrónicas, agrupados en el BEREC (Body of European Regulators for Electronic Communications) especifica:

- Artículo 4: el derecho de todos los usuarios finales (abonados de una operadora) para elegir a un proveedor de servicios de itinerancia internacional diferente al proveedor utilizado en la red local. El proceso se conoce como venta por separado (decoupling) de los servicios de itinerancia internacional.

- Artículo 5: define el derecho de los proveedores alternativos (ARPs) para solicitar los servicios e instalaciones necesarias para ofrecer servicios de itinerancia internacional regulados por separado a los clientes de cualquier proveedor.

Para poder facilitar el cumplimento de estos artículos y facilitar el servicio de itinerancia internacional independientemente del operador de la red local, podemos basarnos en tres tecnologías básicamente, alguna de ellas mencionadas brevemente con anterioridad en el proyecto:

- Local Break-Out (LBO): consiste en la provisión de los servicios de datos cuando el usuario se encuentra en itinerancia internacional por parte de un proveedor de servicios de la red visitada con la única intervención de la red local para la autentificación del usuario. Esta solución está incluida en los estándares 3GPP ya que se diseñó inicialmente para optimizar la gestión del tráfico de datos en itinerancia internacional, pero puede ser utilizada por los operadores de la red visitada para actuar como un ARP dando acceso a Internet y otros servicios de datos a los usuarios y la facturación se haría directamente con ellos.

- IMSI dual: se establecerá una relación permanente entre el usuario y el ARP a través de tarjetas USIM con dos IMSIs, uno para la red local del usuario y el otro rango de IMSIs para cuando se encuentre disfrutando de los servicios de itinerancia internacional en cualquier país miembro de la Unión Europea.

- IMSI único: es una solución menos compleja que el modelo LBO y no sólo para el servicio de datos. Para ello, los ARPs firmarán convenios con cada uno de los operadores de la red visitada para poder ofrecer toda clase de servicios a aquellos clientes potenciales. El flujo de mensajes de dichos servicios es exactamente igual que en los escenarios clásicos de itinerancia internacional, lo que varía es la forma de facturar los servicios, que en este caso se hará en función de los convenios firmados entre el ARP y la operadora del país visitado.

Como hemos mencionado anteriormente, a partir de Junio del 2017, serán abolidos los sobrecostes por el servicio de itinerancia internacional, así que las operadoras deberán afinar al máximo los procedimientos que utilicen para redirigir el tráfico de sus abonados en el extranjero. Además con la inclusión de los proveedores de servicio alternativos

(ARPs) en el mundo de la itinerancia internacional permitiendo al usuario final elegir aquel proveedor que le proporcione mejores precios, afectará directamente al modelo de redirección de tráfico actual que se está realizando en las operadoras. Éstas no podrán aplicar redirección al tráfico de dichos usuarios para permitir que utilice el ARP elegido, así que la configuración del sistema redirector deberá hacerse de forma muy cuidadosa, prácticamente a nivel de abonado para evitar la pérdida de servicio de éstos en las redes visitadas.

Sin embargo las operadoras pueden volcarse de lleno con los problemas asociados de la **itinerancia accidental o itinerancia fronteriza**, es decir, aquellos usuarios que se encuentren en la frontera de su mismo país, pero se registran en una de las redes del país vecino. Normalmente esto ocurre cuando la potencia de la red del país fronterizo es mucho mayor a la de la red propia, provocando que el terminal móvil acabe registrándose en ella. Dicho comportamiento provoca reclamaciones y quejas por parte de los usuarios por la aplicación de las tarifas de itinerancia, generando un gran descontento y desconfianza entre ellos. Los abonados prepago son los usuarios más afectados pues sólo son capaces de detectar este comportamiento una vez el saldo disponible ha sido agotado, pero no disponen de una factura para poder hacer las reclamaciones pertinentes a la operadora.

Se pueden adoptar diferentes medidas para solventar dicho problema:

- Optimización de la potencia y localización de las antenas en la zona fronteriza.

- Ofrecer la posibilidad a los abonados de pedir el bloqueo explícito del servicio de itinerancia internacional cuando se encuentren localizados en la frontera del país.

- La utilización de plataformas **BRG (Border Roaming Gateway),** que a través del tráfico de señalización serán capaces de identificar a aquellos usuarios que se encuentran en una situación fronteriza donde podría ocurrir un caso de itinerancia accidental y actuar de forma adecuada para que no suceda. Esta plataforma supone una nueva funcionalidad que nuestro sistema redirector de tráfico debe asumir para evitar estos casos de itinerancia accidental.

No me gustaría finalizar esta sección de líneas futuras sin mencionar que ahora mismo nos encontramos en el momento en el que las operadoras móviles están comenzando a dar el servicio de voz sobre IP (VoIP). De momento sólo puede ser utilizado entre abonados de la misma operadora, pero en un futuro no muy lejano, comenzarán las interconexiones de redes para ofrecer el servicio de voz sobre IP a sus abonados cuando se encuentran en el extranjero. Supone el fin del ciclo de implementación de la tecnología 4G, que apostaba por una red totalmente IP. A partir de ahora, estaremos expectantes a la próxima generación de comunicaciones móviles, dónde se esperan alcanzar velocidades de 5Gbit/seg reales. La operadora Verizon de Estados Unidos ya se encuentra trabajando en la estandarización y el despliegue de una red comercial para el año 2017.

Glosario

AAA	Authorization, Authentication, Accounting
APN	Access Point Name
ARP	Alternative Roaming Provider
AuC	Authentication Center
AVP	Attribute Value Pair
BEREC	Body of European Regulators for Electronic Communications
BGP	Border Gateway Protocol
BRG	Border Roaming Gateway
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CER	Capabilities Exchange Request
CEA	Capabilities Exchange Answer
CSFB	Circuit Switched Fallback
DCH	Data Clearing House
DEA	Diameter Edge Agent
DPA	Diameter Routing Agent
DPR	Disconnect Peer Answer
DRA	Disconnect Peer Request
DWA	Device Watchdog Answer
DWR	Device Watchdog Request
eNB	Evolved NodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
FCH	Financial Clearing House
GERAN	GSM Edge Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	Groupe Speciale Mobile Associations
GUI	Graphic User Interface
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
HUR	High Usage Report
IDEN	Integrated Digital Enhanced Network
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunications

IOTs	Inter Operator Tariffs
IP	Internet Protocol
IPX	IP Packet Exchange
IRA	International Roaming Agreement
IREG	International Roaming Expert Group
ITU-R	International Telecommunications Union – Radio communication
ITU-T	International Telecommunications Union – Telecommunication
KPI	Key Performance Indicator
LA	Location Area
LAU	Location Area Update
LBO	Local Break Out
LTE	Long Term Evolution
MAP	Mobile Application Part
MCC	Mobile Country Code
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MPLS	Multi-Protocol Label Switching
MSC	Mobile Switching Center
NAS	Non Access Stratum
NRTRDE	Near Real Time Roaming Data Exchange
OC	Open Connectivity
ODB	Operator Determined Barring
OMV	Operador Móvil Virtual
OTA	Over The Air
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
P-GW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
PRD	Permanent Reference Document
PoP	Point of physical Presence
RAT	Radio Access Technology
RNC	Radio Network Controller
RFC	Request For Comment
RADIUS	Remote Authentication Dial-In User Service)
SCTP	Stream Control Transport Protocol
S-GW	Serving Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Control
SMS	Short Message
SoR	Steering of Roaming
SS7	Signalling System 7
TA	Tracking Area
TADIG	Transferred Account Data Interchange Group
TAU	Tracking Area Update
TMSI	Temporary Mobile Subscriber Identity
TDMA	Time Division Multiple Access
UICC	Universal Subscriber Module
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunications Service

UTRAN	UMTS Terrestrial Radio Access Network
UDP	User Datagram Protocol
ULA	Update Location Answer
ULR	Update Location Request
VLR	Visitor Location Register
VoIP	Voice Over IP
VPLMN	Visited Public Land Mobile Network
WiMAX	Worldwide Interoperability for Microwave Access

Referencias

[1] Jose Manuel Huidobro (2012). Comunicaciones móviles. Sistemas GSM, UMTS LTE. Madrid. Editorial RA-MA.

[2] Ramón Agustí, Francisco Bernando, Fernando Casadevall, Ramón Ferrús, Jordi Pérez, Oriol Sallent (2010). LTE: Nuevas tendencias en comunicaciones móviles. Barcelona. Fundación Vodafone España.

[3] 3GPP TS 136.600. LTE, Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Overall description, Stage 2. Versión 12.6.0, release 12 (2015).

[4] 3GPP TS 123.401. LTE, General Packet Radio Service (GPRS) enhacements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access. Versión 12.9.0, release 12 (2015).

[5] RFC 3588. Diameter Base Protocol (2003).

[6] 3GPP TS 123.272. Digital cellular telecommunications system (Phase 2+), Universal Mobile Telecommunications System (UMTS), LTE, Circuit Switched (CS), fallbak in Evolved Packet System (EPS), Stage 2. Versión 11.5.0, release 11 (2013).

[7] GSMA, Roaming [En línea] http://www.gsma.com/publicpolicy/roaming-overview.

[8] GSMA IR.88. LTE and EPC roaming guidelines. Versión 13.1 (2015).

[9] 3GPP TS 129.272. Universal Mobile Telecommunications System (UMTS), LTE, Evolved Packet System (EPS), Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol. Versión 12.7.0, release 12 (2015).

[10] 3GPP TS 123.003. Digital cellular telecommunications system (Phase 2+), Universal Mobile Telecommunications System (UMTS), Numbering, addressing and identification. Versión 12.7.0 (2015).

[11] GSMA IR.80. Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model. Versión 2.0 (2015).

[12] EU Roaming Regulation III. Structual Solutions. High Level Technical specifications. Versión 1.0 (2013).

[13] BEREC Guidelines on Roaming Regulation No 531/2012.

[14] GSMA IR.73. Steering of Roaming Implementation Guidelines. Versión 4 (2014).

[15] GSMA TS 131.102. Universal Mobile Telecommunications System (UMTS), LTE, Characteristics of the Universal Subscriber Identity Module (USIM) application. Versión 12.8.1, release 12 (2015)

[16] 3GPP TS 124.301. Universal Mobile Telecommunications System (UMTS), LTE, Non-Acces-Stratum (NAS), protocol for Evolved Packet System (EPS). Versión 12.9.0, release 12 (2015).

[17] 3GPP TS 123.122. Digital cellular telecommunications system (Phase 2+), Universal Mobile Telecommunications System (UMTS), LTE, Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode. Versión 12.7.0, release 12 (2015).

[18] GSMA BA.30. Steering of Roaming. Versión 4.1 (2014).

Anexo A

Planificación y presupuesto

La duración de este proyecto fin de carrera ha sido de 10 meses. Durante los 9 primeros meses, la dedicación por parte del ingeniero ha sido de ocho horas diarias por jornada laboral y el mes restante, la dedicación ha sido de ocho horas diarias durante todos los días de la semana.

A continuación, describiremos de forma detallada cada una de las fases de las que ha constado este proyecto:

- Fase 1: Familiarización con el entorno de trabajo.

  Previamente a comenzar a trabajar en el proyecto, se debe producir un primer acercamiento al entorno en el que vamos a estar involucrados durante un período largo de tiempo. Herramientas de monitorización, traceo, sistemas de informes y alarmado serán piezas clave en este fase, así como empezar a configurar los DEAs del HUB de roaming. Esta fase ha sido básica para el desempeño en las pruebas realizadas en el entorno de maqueta y producción descritas en el capítulo 6.

  La duración de la fase ha sido de 4 semanas.

- Fase 2: Estudio de las especificaciones de la 3GPP e ITU-T.

A través de las especificaciones técnicas sobre la red LTE, itinerancia internacional y redirección de tráfico, continuaremos con el aprendizaje iniciado en la primera fase. Comenzaremos también con la revisión de la documentación distribuida por el proveedor del sistema redirector.

La duración de la fase ha sido de 4 semanas.

- Fase 3: Conexión directa Hub de roaming y migración de tráfico.

Se iniciará la implementación de la conexión directa al HUB de roaming durante las primeras semanas de esta etapa para poder migrar el tráfico a posteriori. Éste será migrado en diferentes sub etapas, la primera de ellas servirá para comprobar la correcta implementación de la conexión.

La duración de la fase ha sido de 6 semanas.

- Fase 4: Estudio casos previos a la redirección de tráfico.

Durante tres semanas se obtuvieron datos sobre la distribución de los usuarios en las redes visitadas, datos que se utilizarían más tarde para hacer un estudio comparativo.

La duración de la fase ha sido de 3 semanas.

- Fase 5: Análisis de requisitos del sistema redirector.

Estudio de los requisitos que debería cumplir la plataforma de redirección para analizar la viabilidad y los requerimientos necesarios para su implementación.

La duración de la fase ha sido de 3 semanas.

- Fase 6: Pruebas funcionales en entorno de laboratorio y producción.

Revisión de la funcionalidad del sistema redirector tanto en el entorno de laboratorio como en un escenario controlado con tráfico real.

La duración de la fase ha sido de 4 semanas.

- Fase 7: Migración tráfico a la plataforma de redirección y activación.

Etapa muy similar a la realizada durante la migración del tráfico de itinerancia internacional al HUB de roaming. Estará subdividida en dos grandes fases para migrar el tráfico al redirector primero y después activar la redirección de forma secuencial.

La duración de la fase ha sido de 5 semanas.

- Fase 8: Estudio casos tras la redirección del tráfico.

  Tras obtener los datos de distribución de usuarios en las redes tras la aplicación de la redirección, serán utilizados para hacer la comparación entre los escenarios de los que obtuvimos datos con anterioridad.

La duración de la fase ha sido de 4 semanas.

- Fase 9: Documentación.

  Aunque desde el comienzo del proyecto se comenzó a documentar cada una de las tareas y funciones realizadas, es en la parte final cuando se trabaja más intensamente en la redacción de la memoria.

La duración de la fase ha sido de 6 semanas.

El presupuesto del proyecto es presentado a continuación:

AUTOR	Marta López
DEPARTAMENTO	Ingeniería Telemática
TÍTULO	Estudio de un sistema redirector de tráfico de itinerancia internacional en redes LTE
DURACIÓN (MESES)	10
TASA DE COSTES INDIRECTOS	20%
PRESUPUESTO TOTAL DEL PROYECTO (VALORES EN EUROS)	1.217.727,58 €

Hacemos el desglose presupuestario:

PERSONAL					
Apellidos, Nombre	N.I.F	Categoría	Dedicación (Personas mes)	Coste persona mes (€)	Coste (€)
Mario Muñoz	XXXXXXXX	Ingeniero Senior	1	4.289,54	4.289,54
Víctor Corcoba	XXXXXXXX	Ingeniero Senior	1	4.289,54	4.289,54
Marta López	XXXXXXXX	Ingeniero	10	2.694,39	26.943,9
				TOTAL	35.522,98

EQUIPOS *					
Descripción	Coste (€)	% Uso en el proyecto	Dedicación (meses)	Período depreciación (meses)	Coste imputable (€)
Sistema de redirección	500.000	70	7	60	350.000
Sistema de monitorización	600.000	100	10	60	600.000
Simulador de tráfico	125.000	10	1	60	12.500
				TOTAL	962.500

SUBCONTRATACIÖN DE TAREAS *		
Descripción	Empresa *	Coste imputable (€)
Cableado e instalación sistema redirección	XXXX	15.500
TOTAL		15.500

OTROS COSTES DIRECTOS DEL PROYECTO *		
Descripción	Empresa *	Coste imputable (€)
Curso simulador de tráfico	XXXX	500
Curso sistema de redirección	XXXX	750
TOTAL		1.250

(*) La estimación de los costes relativos a los equipos y tareas subcontratadas no es real por motivos de confidencialidad de la empresa. Ocurre lo mismo con el nombre de las empresas que se han encargado de dar formación o realizar alguna tarea en el proyecto.

RESUMEN COSTES	
Costes Directos	
Personal	35.522,98
Amortización	962.500
Subcontratación de tareas	15.500
Costes de funcionamiento	1.250
Costes indirectos	202.954,6
TOTAL	**1.217.727,58**

El presupuesto total de este proyecto asciende a la cantidad de UN MILLÓN DOSCIENTOS DIECISIETE MIL SETECIENTOS VEINTISIETE EUROS CON CINCUENTA Y OCHO CÉNTIMOS

Leganés a XX de Septiembre de 2015

El ingeniero proyectista

Fdo. Marta López Sánchez